Completion of planned inspection at the Ministry of Defence's Audit Corps

Date: 09-07-2019

Decision

Public authorities

The Danish Data Protection Agency has just completed a planned audit at the Ministry of Defence's Audit Corps in October 2018, where the audit had a special focus on the data subjects' rights.

Journal number: 2018-813-0002

Summary

The Ministry of Defence's Audit Corps has been among the authorities selected by the Danish Data Protection Agency in 2018 for supervision in accordance with the Law Enforcement Act [1]. The Danish Data Protection Agency's planned audit of the Ministry of Defence's Audit Corps focused in particular on the data subjects' rights, which are found in section 3 of the Law Enforcement Act.

At the request of the Danish Data Protection Agency, the Ministry of Defence's Audit Corps in the autumn of 2018, in connection with the inspection visit, filled in a questionnaire and submitted this together with additional material to the inspection. The inspection visit took place on 23 October 2018.

In this connection, the Danish Data Protection Agency has noted that the Ministry of Defence's Audit Corps has assessed that at the time of the inspection visit, the Audit Corps has not yet been in a situation where the authority has been obliged to give notice under section 13 (1) of the Law Enforcement Act. 2.

Following the audit of the Ministry of Defence's Audit Corps, the Danish Data Protection Agency finds reason to conclude:

That the Ministry of Defence's Audit Corps has complied with the requirements of the Law Enforcement Act, section 13, subsection. 1.

That notification of defendants in specific military criminal cases will have to take place immediately in accordance with the rules of the Military Administration of Justice Act and thus not the Law Enforcement Act, section 13, subsection. 2, and that the interplay between the Law Enforcement Act, the Military Administration of Justice Act and the Administration of Justice Act is not entirely clear, which is why the Danish Data Protection Agency has on that basis decided to enter into a dialogue with the Ministry of Justice.

That the Ministry of Defence's Audit Corps has not received any requests for insight pursuant to section 15 of the Law Enforcement Act or requests for rectification, deletion and restriction of processing pursuant to section 17 of the Law Enforcement Act.

On this basis, the Danish Data Protection Agency considers the audit to be completed and does not take any further action on that occasion.

A more detailed review of the Danish Data Protection Agency's conclusions follows below.

Duty to provide information

1.1. The duty to provide information pursuant to section 13 (1) of the Law Enforcement Act 1

The Law Enforcement Act, section 13, subsection 1 requires the data controller to make a number of information available to the data subject.

This is the following information:

Identity and contact information for data controllers.

Contact information for the data protection adviser and information about its function in relation to the data subjects.

The purposes of the processing for which the personal data are to be used.

The right to lodge a complaint with a supervisory authority and contact details of the supervisory authority.

The data subject's rights under Chapters 5 and 6 of the Act.

The right to have the competent supervisory authority exercise the data subject's rights in relation to the competent authorities' decisions on omission, postponement, restriction or refusal pursuant to Chapters 4-6, cf. section 40 (1) of the Act. 1, No. 10.

As an example, the Audit Corps has submitted a text on the processing of personal data, which was publicly available on the Audit Corps' website at the time of the inspection visit.

In addition, the Audit Corps has sent a copy of the authority's autoresponder, which is sent automatically to persons who send an email to the authority.

The published website text contains the information required by section 13 (1) of the Act. 1, Nos. 1-6.

In addition, the Auditor Corps has listed in the text some of the information that the authority is obliged to provide in a request for insight, cf. section 15 (1) of the Law Enforcement Act. 2. In connection with the listing, the Auditor Corps has not made it clear that the listing does not deal with all the information that must be provided pursuant to section 15 (1) of the Act. 2.

It is not a requirement under the Law Enforcement Act, section 13, subsection. 1, that the data controller provides information about the information that must be provided in a request for insight, cf. the Law Enforcement Act, section 15, subsection. 2.

If the data controller chooses to list the information that must be provided pursuant to section 15 (1) of the Law Enforcement Act. 2, the data controller should either provide all the information mentioned in the provision or clarify that the listing is only an extract of the information that must be provided.

The Audit Corps has stated that the authority's autoresponder is provided in order to fulfill the duty of disclosure under the Data Protection Ordinance, and that the Audit Corps has in this connection also chosen to provide the information required by the Law Enforcement Act, as the authority sees this as a good service.

It appears from the comments on the draft law on the processing of personal data by law enforcement authorities [2] that the data controller's obligation to make the information available can be fulfilled by making the information available on the competent authority's website or through printed material available to the registered.

It is thus not a requirement that the Auditor Corps provides the information required under the Law Enforcement Act, section 13, subsection. 1, in an autoresponder.

A review of the autoresponder shows that the Auditor Corps has not provided all the information required by the Law Enforcement Act, section 13, subsection. 1 - just like the wording in the autoresponder about e.g. purpose (as opposed to the text on the website) is also not seen to describe all the purposes. At the end of the autoresponder, however, please note that if you want to know more, you can read more about the rules on the Auditor Corps' website www.fauk.dk.

In this connection, the Danish Data Protection Agency must recommend that the Audit Corps either expand the autoresponder with the necessary information required by the Law Enforcement Act, or simply refer to the published text on the authority's website in relation to the Law Enforcement Act - preferably with a direct link to the text. The Danish Data Protection Agency has not assessed whether the autoresponder meets the requirements of Article 13 of the Data Protection Regulation.

1.2. The duty to provide information pursuant to section 13 (1) of the Law Enforcement Act 2

The Law Enforcement Act, section 13, subsection 2, requires that the data controller, when necessary for the data subject to be able to safeguard his interests, must at least give the data subject the following notification:

The legal basis for the treatment.

The period during which the personal data will be stored or, if this is not possible, the criteria used to determine this period.

The categories of any recipients of the personal data, including in third countries or international organizations.

Additional information if necessary, in particular if personal data are collected without the knowledge of the data subject.

The Audit Corps has stated that the Audit Corps has not yet been in a situation where, in the authority's opinion, there has been an obligation to issue a notification pursuant to section 13, subsection 2.

The Audit Corps has stated that it is the authority's assessment that the fact that a data subject has been charged with an infringement does not in itself entail that notification must be given pursuant to section 13, subsection. 2, but that something more is needed.

It appears from the comments on the proposal for a law on law enforcement authorities' processing of personal data [3] that section 13 (1) of the Act. 2 (contrary to section 13, subsection 1) requires that the authority responsible for the data specifically notifies the data subject. In addition, it is stated that notification must be made when necessary, taking into account the specific circumstances in which the information is processed, in order to ensure the data subject a fair processing of the information.

On the other hand, it will not be necessary to notify the data subject if there is a context where the processing of the information cannot lead to negative legal effects for the data subject, or if it must be clear from the context in which the data was collected for the data subject what the information is to be used for, e.g. a person who, for the purpose of a specific investigation, gives an explanation to the police.

Article 18 of the Law Enforcement Directive [4] allows Member States to provide that the exercise of the rights referred to in Articles 13, 14 and 16 - ie. the duty of disclosure, the right of access and the right of rectification, erasure and limitation of processing - shall be implemented in accordance with the national law of the Member States when the personal data are contained in a judgment or register or case file processed in criminal investigations and criminal proceedings.

Recital 49 states that if personal data are processed during a criminal investigation and criminal proceedings, Member States should be able to provide that the exercise of the right to information, access to and rectification or erasure of personal data and the restriction of processing must be carried out in accordance with national rules of procedure. .

In Denmark, the legislature has chosen to regulate the issue in section 18 (1) of the Law Enforcement Act. 3, from which it follows that the rules of the Code of Judicial Procedure and the Military Code of Judicial Procedure on the right to information, access to and rectification or deletion and restriction of processing of personal data in criminal cases apply in relation to rights pursuant to section 3 of the Act.

It appears from the legal remarks to the Law Enforcement Act, section 18, subsection. 3 [5] that the proposed provision thus ensures that the duty of disclosure to the data subject as well as requests for access, correction, deletion or restriction of processing of personal data are handled in accordance with the rules of the Code of Judicial Procedure and the Military Code of Judicial Procedure. Military Code of Judicial Procedure contains rules in this regard.

It appears in the same place in the remarks that the rules of the Code of Judicial Procedure are supplemented by the Military Code of Judicial Procedure with regard to military criminal cases. This means that in such cases it will also be possible to limit the data subject's rights with reference to military security.

In addition, it appears from the legal remarks to the Law Enforcement Act, section 13, subsection. 2 [6] that in the case of personal data contained in a specific criminal case of e.g. the police or the prosecution or in a court decision in a criminal case, the duty to provide information must be carried out in accordance with the rules on notification in the Administration of Justice Act, cf. the proposed section 18, subsection. 3. This means that in these cases the persons in question are notified in accordance with the rules of the Administration of Justice Act. It can e.g. be notification of the accused of the charge, cf. section 752, notification of interference with the secrecy of notification, cf. section 788, or notification of a search, cf. section 798.

It follows from § 1 of the Military Code of Judicial Procedure [7] that in the processing of military criminal cases, the rules of the Code of Judicial Procedure on the processing of criminal cases apply, unless otherwise provided.

It is the Danish Data Protection Agency's assessment that section 18 (1) of the Law Enforcement Act. 3, and the comments thereon do not leave an unequivocal answer to the relationship between the Law Enforcement Act and the Code of Judicial Procedure and the Military Code of Judicial Procedure.

However, the Data Inspectorate's immediate assessment is that the Audit Corps' notification of defendants in specific military criminal cases will have to take place in accordance with the rules of the Military Administration of Justice Act, which in the absence of a special rule refers to the rules of the Administration of Justice Act.

Considering that section 18, subsection 3, and the legal comments are not entirely clear in relation to the interaction between the Law Enforcement Act on the one hand and the Code of Judicial Procedure and the Military Code of Judicial Procedure on the other, the Data Inspectorate has decided to enter into dialogue with the Ministry of Justice in autumn 2018. around here.

The Danish Data Protection Agency must note, however, that in cases where the Audit Corps is obliged to give a notification

pursuant to section 13 (1) of the Act. 2, the authority must of course ensure that the notification is made and that it meets the requirements for this.

1.3 Postponement, limitation or omission of notification pursuant to section 14 (1) of the Law Enforcement Act. 1

It appears from the Law Enforcement Act § 14, paragraph. 1, that notification pursuant to section 13, subsection 2, may be postponed, restricted or omitted if the data subject's interest in becoming aware of the information is found to should give way in order to

avoid obstacles to official or judicial inquiries, investigations or proceedings;

avoid prejudice to the prevention, detection, investigation or prosecution of criminal offenses or the enforcement of criminal sanctions;

protect public safety,

protect state security or

protect the rights of the data subject or others.

The Ministry of Defence's Audit Corps has stated that the authority has never applied section 14, subsection 1, to postpone, limit or omit notification to registered citizens pursuant to section 13, subsection 2.

2. The right of access

2.1. Communication of insights

The rules on the data subject's right of access are set out in Chapter 5 of the Law Enforcement Act.

Pursuant to section 15, subsection 1, the data subject has the right to receive the data controller's confirmation of whether personal data about the person in question is being processed.

If the data controller processes personal data about the data subject, the data controller must give the data subject access to the personal data and a notification with a number of data, cf. section 15 (1) of the Act. 2.

This is the following information:

The purposes and legal basis of the pre-trial.

The affected categories of personal information.

The recipients or categories of recipients to whom the personal data have been transferred, including in particular recipients in third countries or international organizations.

If possible, the intended period of storage or, if that is not possible, the criteria used to determine that period.

The right to request the data controller to rectify or delete personal data or to limit the processing of the data subject.

The right to lodge a complaint with the supervisory authority and the contact details of the supervisory authority.

What personal information is covered by the processing, and any available information on where it comes from.

The Ministry of Defence's Audit Corps has submitted two examples of responding to a request for insight as well as a process description for responding to a request for insight, including a template.

The Audit Corps has stated that the template has been prepared as a response to insights under both the Data Protection Ordinance and the Law Enforcement Act.

The Audit Corps has further stated that the submitted examples were answered in accordance with the Data Protection Ordinance, and that the Audit Corps has generally only received requests for insight in accordance with the Data Protection Ordinance.

As this supervision relates to the rules of the Law Enforcement Act, the Danish Data Protection Agency has only assessed the template on the basis of this set of rules. For the same reason, the Danish Data Protection Agency has not taken a position on the submitted examples.

A review of the template shows that the template was written in response to a person about whom the Auditor Corps only processes personal information on the basis of the request for insight itself and thus not cases where the Auditor Corps otherwise processes information about the request for insight. During the inspection visit, the audit corps stated that a template will be prepared to suit several situations.

In addition, the template only contains information on the right to appeal to the Danish Data Protection Agency and contact information for the Danish Data Protection Agency (§ 15, subsection 2, no. 6) as well as information that the Audit Corps only processes information on requesters - including which - as a result of the request for access (§ 15 (2) (7).

The Danish Data Protection Agency must recommend that the Audit Corps - to the extent that the authority has not already done so - prepare a new template for responding to requests for insight under the Law Enforcement Act, which suits the situations where the authority actually processes information about requests for insight, and also ensures that the template contains the information required under section 15 (2) of the Law Enforcement Act.

The Danish Data Protection Agency must also refer to section 18 (1) of the Law Enforcement Act. 3, as well as the legal

comments thereon, cf. above. In addition, the Danish Data Protection Agency must refer to the statutory comments on section 15 of the Law Enforcement Act [8], which states that in the case of personal data contained in a specific criminal case with e.g. the police or the prosecution or in a court decision in a criminal case, the right of access must otherwise be implemented in accordance with the rules of the Administration of Justice Act on access to the material in criminal cases and on access to court decisions, cf. the proposed § 18, para. Requests for access must thus be decided in accordance with the rules of the Administration of Justice Act in Chapter 3 a on access to documents in e.g. judgments and rulings and the documents in a criminal case as well as §§ 729 a - d on the accused's access to the material in the criminal case. In the case of data subjects whose right of access is not regulated by the rules of the Code of Judicial Procedure, e.g. persons acting as ancillary persons in a criminal case, the rules of the proposed section 3 will apply.

2.2. Postponement, restriction or denial of access pursuant to section 16 of the Law Enforcement Act

It follows from the Law Enforcement Act § 16, paragraph. 1, that the data controller may postpone, limit or refuse to provide insight if the data subject's interest in gaining knowledge of the information is found to give way to the considerations of public interest mentioned in section 14 (1) of the Act. 1.

A decision that the data subject's access is suspended, restricted or denied must be notified to the data subject in writing and must be accompanied by a statement of reasons and a complaint guide, and the decision must include information on the data subject's right to exercise the data subject's competent authority. rights pursuant to section 40, subsection 1, no. 10. This follows from the Law Enforcement Act § 16, para. 2.

The Ministry of Defence's Audit Corps has stated that section 16 (1) of the Law Enforcement Act 1, has not yet been used to postpone, limit or deny access pursuant to section 15 of the Act.

3. Right to rectification, deletion and limitation of processing pursuant to section 17 of the Law Enforcement Act.

The data subject's right to rectification, deletion and limitation of processing is stated in Chapter 6 of the Law Enforcement Act.

It follows from the Law Enforcement Act, section 17, subsection. 1, that the data controller must correct information that turns out to be incorrect. In addition, it is clear from the same provision that the data controller must similarly complete incomplete information if this can be done without jeopardizing the purpose of the processing. In addition, the data controller must notify the competent authority from which the information originates.

Pursuant to section 17, subsection 2, the data controller shall, at the request of the data subject, delete information that has

been processed in violation of the processing rules in Chapter 3 of the Act, or if it is required to comply with a legal obligation to which the data controller is subject.

It follows from section 17 (1) of the Act. 3, that the data controller must instead of deletion limit the processing of personal data if 1) the accuracy of the personal data is disputed by the data subject and their accuracy or inaccuracy cannot be established or 2) the personal data must be retained as evidence. To the extent that a processing is limited, the data controller notifies the data subject before the restriction is lifted, cf. section 17 (1) of the Act. 4.

If the data controller rejects a request for rectification, deletion or restriction of processing, this must be notified to the data subject in writing and must be accompanied by a justification and a complaint guide, as well as information about the data subject's right to have the data subject's competent authority exercise rights in accordance with section 40 (1) of the Act. 1, no. 10. This follows from section 17 (1) of the Act. 5.

The Audit Corps has stated that the authority has not yet received requests for rectification or deletion pursuant to the Law Enforcement Act, just as the authority has not applied section 17 (1) of the Law Enforcement Act. 3, to limit the processing of information instead of deletion.

The Danish Data Protection Agency must - as before - refer to the Administration of Justice Act, section 18, subsection. 3, and the legal comments thereon, cf. above. In addition, the Danish Data Protection Agency must refer to the statutory comments on section 17 of the Act [9], which state that in the case of personal data contained in a specific criminal case with e.g. the police or the prosecution or in a court decision in a criminal case, rectification, etc. of the information is carried out in accordance with the rules in the Administration of Justice Act, cf. the proposal for section 18, subsection 3. This means that a request for rectification of a court decision must be processed in accordance with section 221 of the Administration of Justice Act.

Deadlines and procedures

It appears from the Law Enforcement Act, section 18, subsection. 2, that the data controller shall respond as soon as possible and in writing to requests as mentioned in this section. If the request is not answered within 4 weeks of receipt, the data controller must inform the person concerned of the reason for this and when the request is expected to be answered.

The Ministry of Defence's Audit Corps has stated that the authority expects to be able to respond to all future requests within the deadline.

Prior to the inspection visit, the Audit Corps submitted a process description for requests for insight into personal data as well as guidelines for the processing of personal data both within and outside the criminal justice system, where sections 6.1-6.4 relate to the data subjects' rights. The template for responding to requests for access, which has been reviewed under section 2.1, is an appendix to the process description for requests for access to personal data.

Both the process description and the description of the data subjects 'rights in the guidelines are very generally described, just as they contain a general reference to the fact that employees can seek help and advice from the Audit Corps' data protection adviser.

In addition, the Audit Corps has chosen to prepare the guidelines and the process description in accordance with both the Data Protection Ordinance and the Law Enforcement Act. The confusion has meant that the Audit Corps has not explained the difference between the two sets of rules in relation to the duty to provide information, which has led to an incorrect reproduction of the rules in the Data Protection Regulation. In addition, the Auditor Corps' description of the right of rectification, deletion and limitation is not fully in accordance with the rules.

The Danish Data Protection Agency recommends that the process description and guidelines be elaborated and - where necessary - corrected so that the employees at the authority are equipped to make the ongoing assessments in this regard.

5. Conclusion

Following the audit of the Ministry of Defence's Audit Corps, the Danish Data Protection Agency finds reason to conclude:

That the Ministry of Defence's Audit Corps has complied with the requirements of the Law Enforcement Act, section 13, subsection 1.

That notification of defendants in specific military criminal cases will have to take place immediately in accordance with the rules of the Military Administration of Justice Act and thus not the Law Enforcement Act, section 13, subsection. 2, and that the interplay between the Law Enforcement Act, the Military Administration of Justice Act and the Administration of Justice Act is not entirely clear, which is why the Danish Data Protection Agency has on that basis decided to enter into a dialogue with the Ministry of Justice.

That the Ministry of Defence's Audit Corps has not received any requests for insight pursuant to section 15 of the Law Enforcement Act or requests for rectification, deletion and restriction of processing pursuant to section 17 of the Law Enforcement Act.

On this basis, the Danish Data Protection Agency considers the audit to be completed and does not take any further action on that occasion.

[1] Act No. 410 of 27 April 2017 on law enforcement authorities' processing of personal data with subsequent amendments.

[2] Bill L 168 submitted on 28 March 2017, the special remarks to § 13.

[3] Bill L 168 submitted on 28 March 2017, the special remarks to § 13.

[4] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data by competent authorities for the purpose of preventing, investigating, detecting or prosecuting criminal offenses or enforcing criminal sanctions and on the free movement of such information and repealing Council Framework Decision 2008/977 / JHA.

[5] Bill No. L 168 submitted on 28 March 2017, the special remarks to § 18.

[6] Bill No. L 168 submitted on 28 March 2017, the special remarks to § 13.

[7] Act No. 531 of 24 June 2005 Military Administration of Justice Act with subsequent amendments.

[8] Bill No. L 168 submitted on 28 March 2017, the special remarks to § 15.

[9] Bill No. L 168 submitted on 28 March 2017, the special remarks to § 17.