

Clarification of data liability

Date: 12-08-2019

Decision

Public authorities

The University of Copenhagen is data responsible for the processing of personal data carried out by medical students who, during internships, record their own consultations with a view to fulfilling their obligations for resp. teaching and examination at the University of Copenhagen.

Journal number: 2018-441-0030

Summary

In connection with a case in which a medical student had a video camera owned by the University of Copenhagen, the Danish Data Protection Agency has taken a position on data responsibility when a medical student is in an internship.

On 1 June 2018, the Danish Data Protection Agency received a report from Lægerne Gammel Strandvej about a breach of personal data security. It appeared from the notification that a medical student from the University of Copenhagen - in connection with a 4-week internship at Lægerne Gammel Strandvej - on 25 May 2018 had a video camera with recordings of patients stolen for use at the University of Copenhagen. The camera was owned by the University of Copenhagen.

Subsequently, Bruun Hjejle, on behalf of Lægerne Gammel Strandvej, argued that Lægerne Gammel Strandvej was nevertheless not data responsible for the processing of personal data in question, and instead informed the University of Copenhagen as a possible data controller. On that basis, the Danish Data Protection Agency requested a statement from the University of Copenhagen.

In its decision, the Danish Data Protection Agency emphasized that it is the University of Copenhagen that has established the scheme and the rules for internships for the course in general medicine. The course is part of the medical student's subject at the University of Copenhagen, and it is thus the University of Copenhagen that decides for what purposes and with what aids the processing of personal data may be carried out.

When the Data Inspectorate found that the University of Copenhagen is data responsible for the processing of personal data in question, the Data Inspectorate is of the opinion that the University of Copenhagen - by 1) having lost a video camera containing information about an unknown number of data subjects, including health information, 2) not having reported the

breach of personal data security to the Danish Data Protection Agency and 3) not notifying the registered persons covered by the breach of personal data security has not complied with the requirements of Article 32 (1) of the Data Protection Regulation. 1, artikel 33, stk. 1 and Article 34, para. 1.

Against this background, the Danish Data Protection Agency has expressed serious criticism that the University of Copenhagen's processing of personal data has not taken place in accordance with the Data Protection Ordinance. The Danish Data Protection Agency has noted that the University of Copenhagen was of the opinion that the student was data responsible for the processing of personal data in question, which is the reason why the University of Copenhagen has not acted in accordance with Article 32 (1) of the Data Protection Regulation. 1, artikel 33, stk. 1 and Article 34, para. 1.

Decision

1.

The Danish Data Protection Agency hereby returns to the case where the Danish Data Protection Agency on 1 June 2018 received a report from Lægerne Gammel Strandvej about a breach of personal data security.

Following a review of the case, the Danish Data Protection Agency's opinion, including in particular the University of Copenhagen's statements of 3 April and 6 May 2019, is that the University of Copenhagen is data responsible for the processing of personal data performed by the medical student during the internship at Lægerne Gammel Strandvej.

Following a review of the case, the Danish Data Protection Agency finds grounds for expressing serious criticism that the University of Copenhagen's processing of personal data has not taken place in accordance with the Data Protection Ordinance.

Below is a more detailed review of the case and a justification for the Danish Data Protection Agency's decision.

2. Case presentation

On 1 June 2018, the Danish Data Protection Agency received a report from Lægerne Gammel Strandvej about a breach of personal data security.

It appears from the notification that a medical student from the University of Copenhagen - in connection with a 4-week internship at Lægerne Gammel Strandvej - on 25 May 2018 had a video camera stolen with recordings of patients for use at the University of Copenhagen. The camera is owned by the University of Copenhagen.

By letter dated 9 August 2018, the Danish Data Protection Agency requested the doctors Gammel Strandvej for an opinion on

the case. By letter dated 12 September 2018, Bruun & Hjejle, on behalf of Lægerne Gammel Strandvej, issued a statement on the matter.

In the statement, Bruun & Hjejle argued that Lægerne Gammel Strandvej is nevertheless not data responsible for the processing of personal data in question. At the same time, Bruun & Hjejle came up with a proposal as to who could be responsible for the data in question, and in this connection informed the University of Copenhagen as a possible data controller.

By letter dated 13 March 2019, the Danish Data Protection Agency requested a statement from the University of Copenhagen.

By letter dated 3 April 2019, the University of Copenhagen issued a statement on the matter.

By letter dated 16 April 2019, the Danish Data Protection Agency again requested a statement from the University of Copenhagen. In this connection, the Danish Data Protection Agency requested the University of Copenhagen to fill in the form with questions attached by letter of 13 March 2019. In addition, the Danish Data Protection Agency requested the University of Copenhagen to explain what considerations and criteria the University of Copenhagen has included in the risk-based approach to processing security, as Article 32 (1) of the Data Protection Ordinance. 1, is an expression of.

By letter dated 6 May 2019, the University of Copenhagen issued a renewed statement on the matter.

2.1. Comments from the University of Copenhagen

In its statement to the Danish Data Protection Agency of 2 April 2019, the University of Copenhagen stated that the student is data responsible for the processing of personal data that takes place as part of the participation in courses at the University of Copenhagen, as the students themselves "decide for what purposes and with which aids may be processed personal data ", cf. the definition of the term data controller in Article 4 (1) of the Data Protection Regulation. 1, No. 7.

The University of Copenhagen has stated that the Executive Order on Education, Executive Order no. 1328 of 15 January 2016 on bachelor's and master's programs at the universities, lays down more detailed rules on the purpose and organization of the programs. Section 33 of the Executive Order authorizes the universities to lay down rules for the individual programs. In accordance with section 33 of the Executive Order, the University of Copenhagen has established curricula for the programs that the university offers. The curriculum does not regulate the purpose of the specific collection of information that the students make as part of the participation in the course.

The University of Copenhagen has also stated that, in accordance with section 33, the university lays down rules for

internships in the curricula for the individual programs, whereby rules are laid down for the course in general medicine, which includes an internship. This describes the overall purpose of the course and the internship. In addition, general guidelines are given for the implementation of the internship course in the form of, for example, "Course booklet Spring 2018" regarding the Clinical Course in General Medicine.

The University of Copenhagen guides the student in connection with the completion of the program, cf. section 9 of the University Act. The guidance does not imply that the University of Copenhagen "decides" the purpose of the students' collection of personal data. The University of Copenhagen does not have the same instructional powers towards the students as towards the university employees.

In connection with the health science and health professional educations, it appears from the Health Act, section 41, subsection. 2, no. 7, that healthcare professionals may pass on information about patients without the patient's consent to "a student who, as part of a health science or health professional education, participates in the treatment of a patient without being an assistant". The University of Copenhagen has stated that if the university was responsible for data, the provision would not provide access to a transfer of data to the student.

The University of Copenhagen has stated that the university - in connection with the students' bachelor projects or master's theses - only approves the student's subject delimitation or assignment formulation, the University's approval and subsequent guidance is only a support to the student.

The University of Copenhagen has further stated that the fact that the university has lent a camera to the student cannot mean that the university is responsible for the video material that the student keeps on camera. The university refers to the fact that the "aids" in a processing can be delegated by the data controller with regard to technical or organizational issues. The lending scheme has been established to support the safe collection and storage of patient data, in accordance with Article 32 of the Regulation. The lending scheme can therefore be considered as a delegation of choice of aids as described in the Article 29 Working Party's opinion of 16 February 2010.

In connection with the Danish Data Protection Agency's questions about the extent to which and how the University of Copenhagen makes students aware of their responsibility when processing personal data, the university has stated that information on the handling of personal data in connection with the study is available on the education pages. There is also information about personal data in the teaching on the university's teaching portal targeted at the teachers. In connection with

the university's strategy 2023, the university has launched a project on "Common goals at the University of Copenhagen for digitization of the programs". One of the initiatives has a special focus on "digital education of students", and aims, among other things, on preparing additional information material for students about the personal data rules and information security. The University of Copenhagen has further stated that when the Personal Data Act was in force, students' processing of personal data was covered by the Executive Order on Exemptions, Executive Order no. 410 of 9 May 2012 amending the Executive Order on exemption from the obligation to notify certain processes . The Executive Order on Exceptions stipulated exemptions from the notification obligation for private data controllers pursuant to section 48 of the Personal Data Act. The Danish Data Protection Agency's previous guidelines regarding the Personal Data Act did not state that students could not be data controllers. As the definition of a "data controller" has not been changed, it must be assumed that the interpretation of the term in relation to students, which could be deduced from the Executive Order on Exceptions, can be continued in relation to the corresponding term in the Data Protection Regulation.

In its latest statement to the Danish Data Protection Agency of 6 May 2019, the University of Copenhagen has generally stated that the University of Copenhagen until 16 April 2019 assumed that the student was data responsible for the processing of personal data performed by the medical student. It has therefore not been possible for the University of Copenhagen to account for the considerations and criteria that the University of Copenhagen has included in the risk-based approach to treatment security, as the university has not considered itself responsible for data at the time of the incident and therefore did not conduct a risk assessment. with the student's activities.

The University of Copenhagen has stated that if the University of Copenhagen is considered to be responsible for data, it seems problematic that the university is responsible for activities carried out by persons who are not covered by the university's instructional powers. The University of Copenhagen has stated that no data processor agreement has been entered into with the students who followed the course in general medicine, as the University of Copenhagen has considered the student to be responsible for the data.

Regarding the specific incident, the University of Copenhagen has stated that the student obtains the patient's oral and written consent to participate in a video. The instruction for the student appears from the University of Copenhagen's course booklet, and it is pointed out in the introductory lecture that the course booklet must be read and that confidentiality and security must be taken deeply seriously. The course booklet informs the student that

"You must exercise extreme caution and care with the video recordings. Take care of the camera and the SD card. Only show the video to those who meet the conditions in paragraph 1. (NB: It follows that the video part of the exam is not public, even though exams at the University of Copenhagen are public.). We do not recommend that the videos be copied to your computer, if you do so you are responsible for deleting the copy ".

The admission does not include name or social security number and is kept with the student for the examination (max. 5 weeks). After the examination, the admission to the university is kept for 14 days after the examination in order to meet the appeal deadline for the examination.

The University of Copenhagen has further stated that the university was informed of the breach of the personal data security by the student by e-mail of 25 May 2018, the same day as the camera was stolen. The University of Copenhagen was informed that there was a video with a number of patients, but not about the identity of the patients in question or details about the content. No interview was held with the student.

In addition, the University of Copenhagen has stated that the persons concerned have not been notified, as the university has assessed that the theft was not directed at the personal data and that the probability of misuse was infinitely small. It is not likely that the persons can actually be identified on the basis of the video recording, and there is no risk of identity theft, as neither name nor social security number appears. In this connection, the University of Copenhagen has stated that no measures have been taken to limit the damage suffered by the data subjects in the breach of personal data security, as the University of Copenhagen is not aware of or able to predict what damage the data subjects have suffered. .

The University of Copenhagen has finally stated that the university has not experienced similar breaches of personal data security since the course received its current form in 1993.

Relevant legal rules

The Danish Data Protection Agency may, for information on the Data Protection Regulation [1], state that the Regulation, in accordance with Article 2 (1) thereof, 1 shall apply to the processing of personal data carried out in whole or in part by means of automatic data processing, and to other non-automatic processing of personal data which is or will be contained in a register.

The Danish Data Protection Agency may further state that a data controller, in accordance with Article 4 (1) of the Data Protection Regulation 1, no. 7, is to be understood as a natural or legal person, a public authority, an institution or another

body which, alone or together with others, decides for what purposes and with what aids personal data may be processed; if the purposes and means of such processing are laid down in Union or national law of the Member States, the controller or the specific criteria for its designation may be laid down in Union or national law of the Member States.

A data processor must, in accordance with Article 4 (1), 1, no. 8 is understood as a natural or legal person, a public authority, an institution or another body that processes personal data on behalf of the data controller [...]

Article 32 (1) of the Data Protection Regulation 1, states that the data controller, taking into account the current technical level, the implementation costs and the nature, scope, coherence and purpose of the processing in question, as well as the risks of varying probability and seriousness of natural persons' rights and freedoms, implement appropriate technical and organizational measures to ensure a level of safety appropriate to these risks.

Article 32 (1) of the Regulation 2, it is clear that in assessing the appropriate level of security, particular account shall be taken of the risks posed by processing, in particular in the event of accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to personal data transmitted; , stored or otherwise processed.

It follows from Article 33 (1) of the Data Protection Regulation 1, that breaches of personal data security shall be reported by the controller without undue delay and, if possible, within 72 hours after he has become aware of the breach of personal data security, to the supervisory authority competent in accordance with Article 55, unless this is unlikely; , that the breach of personal data security involves a risk to the rights or freedoms of natural persons. If the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by a reason for the delay.

In addition, it follows from Article 34 of the Regulation that when a breach of personal data security is likely to involve a high risk to the rights and freedoms of natural persons, the controller shall without undue delay notify the data subject of the breach of personal data security.

4. The Danish Data Protection Agency's opinion

4.1. Data responsibility

It is the Data Inspectorate's opinion that the University of Copenhagen is data responsible for the processing of personal data carried out by the medical student during the internship at Lægerne Gammel Strandvej.

The Danish Data Protection Agency has emphasized that the purpose of recording the consultations is that the student can use the recordings to fulfill his obligations for resp. teaching and examination at the University of Copenhagen.

In addition, the Danish Data Protection Agency has emphasized that, in accordance with section 33 of the Executive Order on Education, it follows from the course booklet "Spring 2018 for Clinical Courses in General Medicine" that the University of Copenhagen has determined the scheme and rules for internships for the course in general medicine. . The course is part of the medical student's subject at the University of Copenhagen, and it is thus the University of Copenhagen that decides for what purposes and with what aids the processing of personal data may be carried out. The Danish Data Protection Agency has further emphasized that the instruction for the student appears in the course booklet, and it is pointed out by the University of Copenhagen at the introductory lecture that the course booklet must be read.

In conclusion, the Danish Data Protection Agency has emphasized that there is no disclosure of information where the Health Act, section 41, subsection 2, no. 7, applies and that the processing relevant to the security breach can be isolated for processing in the form of recording and storage of personal data on a video camera owned by the University of Copenhagen for use in the student's obligations for resp. teaching and examination at the University of Copenhagen. In this connection, the Danish Data Protection Agency has emphasized that the University of Copenhagen's "Cooperation and Confidentiality Agreement" states that personal data for the project may only be stored and processed on computers and other research equipment belonging to the University of Copenhagen.

The Danish Data Protection Agency has noted that the University of Copenhagen has not taken a position on the risks that the processing of personal data entails for the data subjects, as it has so far been the University of Copenhagen's assessment that the individual student was data responsible for the processing of personal data. of the medical student in internship.

As stated above, however, the Danish Data Protection Agency's assessment is that the University of Copenhagen is data responsible for the processing of personal data carried out by medical students during internships.

The Danish Data Protection Agency must therefore recommend that the University of Copenhagen assess the risks that the processing entails for the data subject, as in the Data Inspectorate's opinion this is a prerequisite for implementing appropriate technical and organizational measures pursuant to Article 32 (1) of the Data Protection Regulation. 1.

4.2. Treatment safety

The Danish Data Protection Agency finds that the storage of recordings of patients is a processing of personal data that is covered by Article 2 (1) of the Data Protection Regulation. 1.

The Danish Data Protection Agency has emphasized that the information in question, despite the fact that neither name nor

social security number appears, is sufficiently specific to be able to identify a person, and that it thus also appears to unauthorized persons as information about a specific natural person, cf. Judgment of the European Court of Justice C-434/16, paragraph 35.

It is the Danish Data Protection Agency's assessment that personal data in connection with medical consultations constitute personal data on health covered by the special categories of personal data, cf. Article 9 (1) of the Data Protection Regulation. 1.

After a review of the case, including that the University of Copenhagen is data responsible for the processing of personal data, it is the Data Inspectorate's opinion that the University of Copenhagen - by losing a video camera containing information about an unknown number of data subjects, including health information - has not lived up to the requirement to implement appropriate security measures in accordance with Article 32 (2) of the Data Protection Regulation; 1.

In this connection, the Danish Data Protection Agency is of the opinion that the University of Copenhagen should have established measures with a view to securing the information in question against it coming to the knowledge of unauthorized persons, e.g. through encryption of the storage medium (SD card), separate storage of the storage medium separate from the camera or similar measures to make the information inaccessible to unauthorized persons.

In addition, the Danish Data Protection Agency has emphasized that the recordings were made in connection with medical consultations, which is why the breach of personal data security concerns health information. There is therefore a high risk to persons' rights or freedoms, as exposure of the recordings may entail a breach of integrity for the persons in question, just as it may also have social consequences for the data subjects.

After a review of the case, the Danish Data Protection Agency also finds that the University of Copenhagen - by not reporting the breach of personal data security to the Danish Data Protection Agency - has not complied with the requirement to report breaches of personal data security without undue delay and if possible, no later than 72 hours after the data controller. has become aware of the breach in accordance with Article 33 (1) of the Data Protection Regulation. 1.

Following a review of the case, the Danish Data Protection Agency also finds that the University of Copenhagen - by not notifying the registered persons covered by the breach of personal data security - has not acted in accordance with Article 34 (1) of the Data Protection Regulation. 1.

On this basis, the Danish Data Protection Agency finds grounds for expressing serious criticism that the University of

Copenhagen's processing of personal data has not taken place in accordance with the Data Protection Ordinance.

The Danish Data Protection Agency has also emphasized that the University of Copenhagen was informed of the breach of personal data security on 25 May 2018, when the breach occurred, but subsequently did not take any further action in connection with it.

The Danish Data Protection Agency does not consider the information provided by the University of Copenhagen that the theft was not aimed at personal data and that the University of Copenhagen is not aware of or able to predict what damage the data subjects have suffered to be relevant to the case.

The Danish Data Protection Agency has noted that the University of Copenhagen was of the opinion that the student was data responsible for the processing of personal data in question, which is the reason why the University of Copenhagen has not acted in accordance with Article 32 (1) of the Data Protection Regulation. 1, artikel 33, stk. 1 and Article 34, para. 1.

5. Concluding remarks

In view of the nature of the case, the Danish Data Protection Agency must state that the University of Copenhagen must not make a separate notification of the breach of personal data security, cf. Article 33 (1) of the Data Protection Ordinance. In this connection, the Danish Data Protection Agency has emphasized that the breach has been sufficiently elucidated in connection with the processing of the case in the audit, and that the University of Copenhagen has otherwise acknowledged the course of the case.

The Danish Data Protection Agency regrets the long case processing time due to great busyness in the audit, just as the audit regrets that the University of Copenhagen has not been continuously informed about delays in the case processing time, etc.

A copy of this letter is sent today to Bruun Hjejle for information.

[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 the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (General data protection regulation).