Critical conditions at the Statens Serum Institut's COVID-19 modeling project

Date: 25-03-2021

Decision

Public authorities

On the basis of a case taken up on its own initiative, the Danish Data Protection Agency expresses serious criticism of the Statens Serum Institut for initiating processing of personal data without adequate risk assessment, impact analysis, consultation with the Danish Data Protection Agency, data processor agreements and appropriate security measures.

Journal number: 2020-432-0044

Summary

In connection with the escalation of the COVID-19 situation in Denmark (February-March 2020) and the subsequent closure of society, the Statens Serum Institut (SSI) was to make personal data - in the form of, among other things, health information - available to an expert group that was to calculate on possible scenarios for reopening.

SSI itself had assessed that the risk for the data subjects was moderate to high and found that at the start of the treatment, a complete mapping and assessment of the risks involved in the treatment had not been carried out. SSI assessed that this in itself entailed a high risk to the data subjects' rights.

However, the originally intended IT solution for the data exchange could not be ready fast enough, which is why the data access in week 12 was established on SSI's SFTP server, located behind an external firewall in a zone that could be accessed by outside experts (also called DMZ). The information was located in dedicated directories, where the experts who were to have access used usernames and passwords.

SSI has stated that the risk assessment due to lack of internal resources and the situation at the time was only started in week 16, and that the first version of an impact assessment was available in week 17. Data processor agreements with the expert group members were also signed in week 17.

At the end of 2019, SSI began an upgrade in the field of data protection. In February-March 2020, there were two positions for compliance (one was vacant, however). There were upgrades with an additional eight positions to start on April 1st. SSI has stated that they used external assistance when they found that they were missing employees.

The Danish Data Protection Agency found that SSI already at the time when they - before the commencement of processing -

had realized that this entailed a high risk to the data subjects' rights, should have started work on the impact assessment. This especially when it was clear that it was urgent to get started with the treatment. The Authority also found that - when there is a built-in high risk for the data subjects' rights - and this risk has not been reduced through the initiatives that should actually arise from an impact assessment, it is only possible to start processing once the Data Inspectorate has been consulted.

The Danish Data Protection Agency found that the necessary data processor agreements were not entered into until five weeks after the commencement of processing.

In addition, the Danish Data Protection Agency found that in choosing the temporary solution on SSI's SFTP server, the risk of unauthorized access to the information had not been taken into account, especially assessed in relation to the nature, interest and abilities of the information among those actors who might be interested in it. , and the technical nature of the solution chosen. The Authority therefore found that the solution did not have the required level of security.

The Danish Data Protection Agency found that it was mitigating circumstances that the processing should be established during an international crisis situation, that there was a significant societal interest in the rapid execution of the processing, and that SSI - however - had considered the temporary deviation from the data protection rules and - to some extent - had tried to remedy these.

Against this background, the sanction was set solely for serious criticism.

In general, the Danish Data Protection Agency is of the opinion that non-compliance with the legal protections that the regulation presupposes in order to reduce high risks in a given processing, and that initiating such processing without consulting the supervisory authority, is a violation of considerable seriousness. Especially since such a method undermines the guarantee that the supervisory authority assesses the full legality of the processing and that no illegal processing with a high risk to the rights of the data subjects is initiated. The sanction provided for in this case must be seen only in the light of the absolutely extraordinary situation which prevailed at the time in question for the specific treatment.

Decision

The Danish Data Protection Agency hereby returns to the case where the Authority - on the basis of an inquiry from the Ministry of Health and the Elderly - has chosen to investigate the Statens Serum Institut's (SSI) processing of personal data in connection with the COVID modeling project.

The Danish Data Protection Agency initially notes that the Danish Data Protection Agency understands the acute crisis

situation that existed in the period around week 12 2020, and which SSI was in at the time prior to the start of the processing of personal data for use in elucidating the development of COVID-19 in Denmark. The Danish Data Protection Agency also understands that there was a significant societal interest in following the development. It is important to point out, however, that the Danish Data Protection Agency has an expectation that an institution such as SSI, which for many years has carried out several treatments that include a large number of citizens' health information, has significant experience with data protection law issues, and that this is also in more acute situations.

Decision

Following a review of the case, the Danish Data Protection Agency finds that there are grounds for expressing serious criticism that SSI's processing of personal data has not taken place in accordance with the rules in Article 28 (1) of the Data Protection Regulation. 3, artikel 32, stk. 1, artikel 35, stk. 1, and Article 36, para. 1.

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

2. Case presentation

On 10 June 2020, the Danish Data Protection Agency received an inquiry from the Ministry of Health and the Elderly. In the inquiry, the Ministry of Health and the Elderly informed the Danish Data Protection Agency of a memorandum from SSI, dated 15 May 2020, regarding SSI's deviation from certain provisions in the Data Protection Regulation in connection with the COVID modeling project.

On 6 August 2020, the Danish Data Protection Agency issued a statement in the case and asked SSI for an account of the course of events.

Against this background, on 27 August 2020, SSI sent a statement to the Danish Data Protection Agency with information on the course of events and a copy of the department's risk assessment and impact assessment.

The Danish Data Protection Authority then decided to investigate SSI's processing of personal data in connection with the COVID modeling project, and why the Authority on 28 September 2020 requested SSI for an opinion for the purpose of processing the case.

On 12 October 2020, SSI issued a statement on the matter.

2.1. SSI's comments

Regarding the COVID modeling project in general, SSI has stated that in connection with the escalation of the COVID-19

situation in Denmark and the subsequent closure of society, SSI was asked to set up an expert group to carry out a large number of statistical studies, the results of which were decisive for elucidation of the development of COVID-19 as well as the effect of the authorities' measures to limit the spread of infection in society, including an analysis of the pace at which society could “reopen”. SSI was asked by the Ministry of Health and the Elderly to start work immediately and to give the expert group access to the initial data sources that SSI already dealt with in connection with SSI's authority task.

SSI began processing personal data in week 12 before a sufficient contractual basis had been prepared between SSI and the expert group, and before a risk assessment and impact assessment had been prepared. This was done on the basis of a balance between the need for rapid delivery of analyzes due to the acute and serious nature of the situation in relation to the health and economic consequences for Denmark and the requirement for documented data protection law compliance.

The information at this time consisted primarily of information about COVID-19 sample data, hospital occupancy relative to COVID-19, and information about early symptoms, which by 1813 were categorized as influenza-like symptoms. In addition, anonymous aggregated information was entered as parameters in the mathematical calculations.

At the beginning of the project, all potential risks had not yet been fully elucidated, including whether there were any high risks, which according to SSI in itself constituted a high risk.

The risk for the data subjects was assessed as moderate to high.

2.1.1.

Regarding the expert group's access to personal data, SSI has stated that SSI generally uses Forskermaskinen at the Danish Health and Medicines Authority (SDS) or Statistics Denmark for processing personal data in connection with scientific and statistical surveys, etc., and that it was intended from the beginning that the project should be based on Forskermaskinen at SDS or a similar safe analysis environment.

However, there was a need to start processing immediately and give the expert group access to process the information before SSI, in collaboration with SDS, could establish an environment for the project at Forskermaskinen.

A temporary solution was therefore prepared until the project could be moved to Forskermaskinen, where the relevant people from the expert group from 21 March 2020 (Sunday in week 12) gained access to personal information in pseudonymised form via a dedicated model group folder on SSI's sFTP server . At the same time, work was being done to enter into data processor agreements with the expert group's external parties, which was delayed due to several factors, e.g. lack of internal resources

at SSI.

However, there were significant challenges in establishing a suitable environment at Forskermaskinen, which is why the temporary solution had to last longer than planned.

The data processor agreements with the expert group were designed so that they could include both the current solution and the future solution on Forskermaskinen and were signed in week 17.

When the project was moved to Forskermaskinen, in accordance with the data processor agreements, deletion was initiated by data processors who had had access to personal information at the sFTP server.

2.1.2.

Regarding the preparation of a risk assessment in connection with the project, SSI has stated that the work with the risk assessments at the start of the project has been challenged by the COVID-19 situation, which both made communication difficult and affected the amount of SSI's internal resources.

On an ongoing basis with the establishment of the environment at Forskermaskinen at SDS, SSI prepared the first draft of a risk assessment for the project. This was available in week 17, but the work on the risk assessment began in week 16. SSI began with the assistance of an external consultant immediately updating the risk assessment in a version 0.3, which was available in week 18, as SSI did not have the necessary resources seen in connection with the situation the entire Ministry of Health and the Elderly and especially SSI was in connection with COVID-19. SSI worked continuously to identify new risks and implement security measures in line with the project's development, and SSI continues to use the risk assessment as a tool in connection with the project.

2.1.3.

Regarding the use of the sFTP server, SSI has stated that SSI has addressed the risk of using the sFTP server in the risk assessment.

In the impact assessment, SSI has also specifically assessed the risk for the data subjects in connection with the processing of personal data in the period prior to the transition to Forskermaskinen.

It is SSI's assessment that the use of the sFTP server for the processing of personal data constituted an appropriate security measure. SSI has i.a. in the assessment emphasized that the purpose of using the sFTP server was to receive, store and provide access to pseudonymised personal data while observing appropriate security measures.

In this connection, SSI has noted that SSI, taking into account the nature of the personal data, chose to use a dedicated sFTP server rather than a regular FTP server. The solution used was approved by the Ministry of Health and the Elderly's security department for the processing of sensitive personal data.

SSI has further stated that the sFTP server is located in SSI's DMZ, that data is encrypted in up and download, [Extracted here in the decision description of product selection and functionality].

Furthermore, the administrators of the sFTP server have, using dedicated directories on the sFTP server, ensured that only relevant datasets were shared with the expert group.

In addition to the measures set out in the risk assessment and the impact assessment, SSI has implemented the following measures:

Limiting the number of users and access rights

Pseudonymisation of personal data after SSI's fixed process

Implementation of policies, guidelines and procedures as set out in SSI's letter of 27 August 2020

Involvement of SSI's data protection adviser

Advice and assistance from the Chamber Advocate

Allocation of internal resources to the project

Establishment and maintenance of ongoing dialogue between SSI Compliance, project participants and data processors

In relation to the use of the Research Machine, SSI has stated that it has been politically decided that the processing of personal data for scientific and statistical purposes should take place using research machines. The use of research machines is part of the political agreement "Better health through modern and secure use of data" from 2017, of which it i.a. appears: "In the field of research, the physical transmission / viewing of data must be avoided as far as possible, and, for the greatest possible extent, eg pseudonymised data must be used through increased use of secure research machines".

It is thus SSI's position that the processing of personal data in such a form as the project should, as far as possible, take place on a so-called research machine.

It is SSI's assessment that the sFTP server does not contribute with the same degree of inherent security measures as is the case with Forskermaskinen in the form of functionality, IT environments, creation process for projects, monitoring, etc.

The research machine has the following inherent safety precautions:

Central management of user access and rights

Central Control of applications and systems that can be used for processing data sets and register data

VPN login to the set up IT environment for the project

Automatic deletion of projects containing data at project expiration

2.1.4.

Regarding the handling of data protection law issues in SSI, SSI has stated that at the time of the project's start-up, SSI had one lawyer to handle data protection law matters who were fully engaged in COVID-19 related processing activities. SSI had also had an additional lawyer in the field, but at the beginning of 2020 the position was not filled. The two lawyers, together with SSI's other two lawyers and the IT security function, performed tasks in relation to data protection. In addition, a CISO was employed at the time the project began.

Recognition of the real extent of the need for more resources to strengthen data protection and information security at SSI arose continuously from May 2018 onwards, and in 2019 SSI decided that the data protection area should be strengthened. SSI continues to reassess the need.

The background for the decision was that in 2019 it was clear that the area needed to be better organized and further strengthened in the form of additional hiring and the creation of a new compliance section if SSI was to achieve a satisfactory level of compliance in terms of data protection and information security. The decision on further recruitment was finally made on December 17, 2019, and organization of the department and hiring of additional staff began thereafter.

For this reason, 8 additional people were recruited starting on 1 April 2020. However, the closure of the community meant that the new employees, like the rest of the country, were repatriated and thus could not physically start on Campus. Certain employees were affected by the fact that day care institutions and schools were closed until after Easter, when the first phase of reopening began.

Thus, at the time of the project's commencement, SSI did not contest sufficient resources to service the project with such a short deadline, and SSI therefore chose to obtain legal assistance from the Chamber Advocate, who allocated 8 lawyers to SSI to assist with COVID-19 projects.

2.1.5.

Regarding the preparation of an impact assessment, SSI has stated that the department has assessed that there was a need

to prepare an impact assessment regarding the processing of personal data in connection with the project.

The unresolved issues that arose in relation to whether the Research Machine could honor the computing power that was needed delayed the impact assessment. SSI decided to complete the impact assessment based on the existing solution. The first version of the impact assessment was available in final form in week 17. SSI immediately began updating the impact assessment in a version 2, which was available in week 20, where i.a. conditions regarding the use of the Research Machine were described and assessed. In addition, SSI worked continuously with evaluation of the course in the intervening period up to the transition to Forskermaskinen in relation to the risk for the registered person. The latest version of the impact assessment was at the time of SSI's statement from week 27.

In this connection, SSI has stated that the project has developed continuously, including in relation to the inclusion of new data sources, and that mitigating measures have been implemented.

Although there was no final impact assessment prior to the start of treatment activity, SSI has been working since week 16 in connection with the use of the risk assessment model for the healthcare sector to identify and assess risks for the data subjects, and the following procedures and guidelines have been implemented:

Procedure for regular assessment of proportionality and assessment of new data sets (prepared for the expert group) Internal procedure for regular assessment of proportionality and assessment of new data sets

Instructions for using the video link (prepared for the expert group)

Internal procedure for passing on information

Instructions for passing on information (prepared for the expert group)

Internal deletion procedure

Guidance regarding. use of the Research Machine

Procedure for supervision of suppliers

Justification for the Danish Data Protection Agency's decision

3.1. Article 32 (1) of the Data Protection Regulation 1

In accordance with the information provided by SSI, the Danish Data Protection Agency assumes that SSI had not fully elucidated all potential risks during the start of the project, which according to SSI in itself constituted a high risk, and that SSI generally assesses that the risk for those registered in connection with the project is moderate to high.

Furthermore, in accordance with the information provided by SSI, the Danish Data Protection Agency assumes that SSI did not have the necessary internal resources to service the project with such a short deadline, including to prepare data processor agreements, risk assessment and impact analysis before the project commences. personal information in connection with the project in SSI's assessment should have occurred on Forskermaskinen from the beginning of the project.

In addition, in accordance with what SSI explained, the Danish Data Protection Agency assumes that both the sFTP server and the data have been located in DMZ.

It follows from Article 32 (1) of the Data Protection Regulation 1, that the data controller must take appropriate technical and organizational measures to ensure a level of security that is appropriate to the risks involved in the data controller's processing of personal data.

Thus, the data controller has a duty to identify the risks that the data controller's processing poses to the data subjects and to ensure that appropriate security measures are put in place to protect the data subjects against these risks.

The Danish Data Protection Agency finds that SSI, by starting the processing of personal data on a set-up that in SSI's initial assessment was not suitable for the processing, could only deviate from this assessment if the temporarily chosen solution constituted appropriate security measures. It is the Data Inspectorate's assessment that the chosen sFTP solution, especially in its placement of data in the DMZ, conditions regarding access control, the nature and number of the information, and the real risk of unauthorized interest in the data in question, did not constitute an appropriate security measure. compared with the fact that SSI states that it has not had the necessary resources allocated to handle data protection law assessments in a timely manner in the process. The Danish Data Protection Agency therefore finds that SSI has not complied with Article 32 (1) of the Data Protection Regulation. 1.

The Danish Data Protection Agency has emphasized that SSI at the beginning of the processing assessed that the lack of coverage of all potential risks constituted a high risk, and that SSI has generally assessed that the processing entails a moderate to high risk for the data subjects, which compared with that this is health information about a significant number of data subjects, should have led to SSI being able to implement a security level appropriate to the assessment from the start of treatment.

The Danish Data Protection Agency has also emphasized that SSI stated that SSI did not have the necessary internal resources before the project began to service the project, including to prepare data processor agreements, risk assessment

and impact analysis, which is why these were only prepared after the processing of data in the project. commenced.

In addition, the Danish Data Protection Agency has emphasized SSI's assessment that processing of personal data in connection with the project from the beginning should have taken place at Forskermaskinen.

The Danish Data Protection Agency is of the opinion that all information and systems placed in a DMZ are potentially exposed to external access attempts. Furthermore, the Authority is of the opinion that given the SSI's status as a research institution, the worldwide awareness of data on COVID-19 and the real threats to unauthorized access, including the high risk to data subjects identified by SSI, it should at least have led to that the information had been placed on the inside of a firewall that only provided access for a limited number of users, possibly verified at given IP addresses or on the basis of a certificate or other qualified credential.

Against this background and after an overall assessment of the information provided regarding the processing of personal data in connection with the project, the Danish Data Protection Agency finds that SSI has not introduced appropriate technical and organizational measures in accordance with Article 32 (1) of the Data Protection Regulation. 1.

The Danish Data Protection Agency has noted that SSI has subsequently introduced organizational and technical measures, e.g. in the form of additional employment in the field of data protection law, and transfer of the project to Forskermaskinen in accordance with the prepared risk assessment and the mitigating measures listed in the subsequent impact assessment.

3.2. Article 35 (1) of the Data Protection Regulation 1 and Article 36, para. 1

It appears from the case that SSI already before the commencement of the processing assessed that the processing entailed a high risk for the data subjects and that there was a need to prepare an impact assessment regarding the processing of personal data in connection with the project.

It also appears from the case that the impact assessment was available in final form in week 17, and that the impact assessment is continuously updated as the project develops.

It follows from Article 35 (1) of the Data Protection Regulation 1, that if a type of processing, in particular through the use of new technologies and by virtue of its nature, scope, context and purpose is likely to involve a high risk to the rights and freedoms of natural persons, the data controller shall carry out an analysis of the intended processing activities. consequences for the protection of personal data.

Furthermore, it follows from Article 36 of the Data Protection Regulation that the controller consults the supervisory authority

before processing, if an impact assessment on data protection carried out in accordance with Article 35 shows that the processing will lead to high risk in the absence of measures taken by the controller to limit the risk. Such an impact assessment must always be carried out before starting treatment.

The Danish Data Protection Agency is of the opinion that SSI should have already begun the preparation of an impact assessment already in the determination of the high risk, knowing that it was important to start the treatments quickly. If SSI was of the belief that such could not be carried out before the commencement of processing, the processing could only have taken place in compliance with the principles set out in Article 36 of the Data Protection Regulation.

As stated, the Danish Data Protection Agency understands that there was a significant societal interest in the processing being started quickly. However, the Authority is of the opinion that in the period from the high risk, and until the treatment was started, it should have been possible for an actor such as SSI, which has countless treatments with sensitive data and inherently high risks, that find that the conditions of Articles 35 and 36 were met, in particular with regard to the choice of a recognized less secure solution.

In particular, the Danish Data Protection Agency has included in its assessment that the purpose of an impact assessment is to determine the specific risks involved in the processing of the data subjects' rights and freedoms and thus ensure that, before commencing processing, measures are established to mitigate these risks and reduce the risk to a level less than high.

By - in a situation where a high risk for the data subjects' rights was recognized - not having prepared an impact assessment before the commencement of processing, SSI has acted in violation of Article 35 (1) of the Data Protection Regulation. 1.

By failing to contact the Danish Data Protection Agency in finding that the lack of measures entailed that the processing had a high risk to the data subjects' rights and freedoms and yet to commence the processing with the inherently high risk, SSI also acted in violation of Article 36 of the Data Protection Regulation. PCS. 1.

The Danish Data Protection Agency has placed particular emphasis on the fact that the protection consideration in Article 36 is that a data controller does not commence processing that has recognized unjustified high risks to the data subjects' rights without consulting the competent supervisory authority first.

The Danish Data Protection Agency has noted that SSI has subsequently prepared an impact assessment.

3.3. Article 28 (1) of the Data Protection Regulation 3

Based on the information in the case, the Danish Data Protection Agency assumes that SSI has assessed that the expert

group's external parties in connection with the project have processed personal data as data processors for SSI.

The Danish Data Protection Agency also assumes that from 21 March 2020, the expert group has had access to process personal data, and that data processing agreements were not entered into until week 17 2020.

It is clear from Article 28 (2) of the Data Protection Regulation 3, that the processing of a data processor shall be governed by a contract or other legal document in accordance with EU law or the national law of the Member States, which is binding on the data processor with respect to the data controller and which determines the subject and duration of the processing; nature and purpose, the type of personal data and the categories of data subjects and the obligations and rights of the data controller

On the basis of the above, the Danish Data Protection Agency finds that SSI, by not having entered into data processor agreements with its data processors from the beginning of the project, has acted in violation of Article 28 (1) of the Data Protection Regulation. 3.

The Danish Data Protection Agency has noted that SSI has subsequently entered into data processor agreements with the department's data processors in the project in question.

3.4. Summary

On the basis of the above, the Danish Data Protection Agency finds that, overall, there are grounds for expressing serious criticism that SSI's processing of personal data has not taken place in accordance with the rules in Article 28 (1) of the Data Protection Regulation. 3, artikel 32, stk. 1, artikel 35, stk. 1, and Article 36, para. 1.

When choosing a sanction in an aggravating direction, the Danish Data Protection Agency has emphasized the nature and scope of the processing, and that SSI, as an experienced player in the field, must be expected to have significant experience in resolving data protection law issues such as those in the case.

In a mitigating direction, the Danish Data Protection Agency has emphasized that the processing took place in connection with a crisis situation, that there was a significant societal interest in the rapid implementation of the processing, and that SSI - however - has considered the temporary deviation from the data protection rules and - to a certain extent - have tried to remedy the derogations. In addition, SSI has subsequently made organizational adjustments to compliance with the Data Protection Ordinance and assisted the Danish Data Protection Agency in clarifying the facts of the case.