Decision regarding the National Police's processing of teledata information

Date: 19-07-2021

Decision

The Danish Data Protection Agency hereby returns to the case where, in June 2019, the Authority on its own initiative initiated an investigation into the National Police's processing of teledata information.

Journal number: 2019-819-0003

Summary

The Danish Data Protection Agency has investigated the processing of personal data by the National Police on the basis that the Authority became aware via press release that an IT system for use in processing information about natural persons' geographical location on the basis of mast information, etc., has not always provided accurate results.

The Danish Data Protection Agency has now completed the processing of the case and expresses serious criticism that the processing of personal data has not taken place in accordance with a number of provisions in the Law Enforcement Act, which is the relevant set of rules when it comes to police processing of personal data. At the same time, the Danish Data Protection Agency issues an order to the National Police to delete the personal data that meets the requirements for deletion in accordance with the telecentre's own guidelines, to the extent that this has not already happened.

The decision is based on the factual circumstances that are already known through the statements that the National Police and the Attorney General gave to the Ministry of Justice, and which the National Police has also sent to the Danish Data Protection Agency in response to the Authority's inquiries.

The Danish Data Protection Agency's investigation is based on the fact that the Authority, through press coverage, became aware that an IT system at the National Police for use in processing information about natural persons' geographical location on the basis of mast information, etc., has not always provided accurate results.

Decision

After a review of the case, the Danish Data Protection Agency finds that there are grounds for expressing serious criticism that the National Police's processing of personal data has not taken place in accordance with the Law Enforcement Act [1] § 27, § 4, para. 4-6 and § 4, para. 8, cf. 7.

The Danish Data Protection Agency also finds grounds for issuing an order to the National Police to delete the personal data

that meet the requirements for deletion in accordance with the telecommunications centre's own guidelines, to the extent that this has not already been deleted.

The order is issued pursuant to section 42 (1) of the Law Enforcement Act. 1.

The deadline for compliance with the order is 6 weeks from today's date. The Danish Data Protection Agency must request to receive a confirmation that the National Police has sufficiently deleted the personal data in question.

The Danish Data Protection Agency draws attention to the fact that according to the Law Enforcement Act, section 50, subsection 2 shall be punished by a fine for failing to comply with an order issued in accordance with section 42.

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

2. Case presentation

By e-mail of 18 June 2019, the Danish Data Protection Agency requested the National Police to report on the processing of personal data in question, including a review of all matters concerning the inclusion of criteria for the processing and presentation of data that the result of the processing expresses. The Danish Data Protection Agency requested to receive the statement no later than 2 July 2019.

By e-mail of 24 June 2019, the National Police requested that the deadline for submitting the statement be postponed to 15 August 2019, as the case was due to a further investigation in coordination with e.g. the individual police districts and the Attorney General. The Danish Data Protection Agency complied with the request for an extension by e-mail of 25 June 2019.

By letter dated 2 July 2019, the Ministry of Justice subsequently requested the National Police and the Attorney General to send a comprehensive statement covering all relevant matters in the teledata case, no later than 6 September 2019, including:

An account of the actual course of the case, including the briefing of the defenders and the courts, and of the time course in relation to the holding of the parliamentary elections on 5 June 2019.

An account of how pending criminal cases have been handled.

An account of the procedure in connection with the collection of telecommunications information in criminal cases.

An account of the control and quality assurance of telecommunications information obtained.

An account of how telecommunications information is used by the police and the prosecution during the investigation and criminal proceedings, including how the prosecution continuously ensures compliance with the principle of objectivity.

It also appeared from the letter from the Ministry of Justice that the statement from the National Police and the Attorney

General would subsequently be included in the ministry's own statement to the Folketing.

As the National Police and the Attorney General's joint statement to the Ministry of Justice included all relevant matters in the teledata case, including the matters that were the subject of the Data Inspectorate's request, the National Police found it most appropriate that the statement requested by the Data Inspectorate be submitted at the same time. Ministry of Justice. The National Police therefore requested an extension of the deadline for submitting the report to the Danish Data Protection Agency to the time when the National Police's report was to be submitted to the Ministry of Justice. This was confirmed by the Danish Data Protection Agency by e-mail of 20 August 2019.

The deadline for the National Police and the Attorney General's joint statement to the Ministry of Justice was subsequently - due to a new development in the case - extended to be received by the Ministry no later than the end of September 2019. The Data Inspectorate agreed by telephone on 27 September 2019. could be postponed until the time when the Ministry of Justice submitted the overall statement to the Folketing.

By letter dated 4 October 2019, the Danish Data Protection Agency received a copy of the National Police and the Attorney General's joint statement to the Ministry of Justice. The letter from the National Police was also accompanied by a note on the National Police and the Attorney General's considerations and new initiatives on the basis of the telecommunications data case and an independent investigation of the National Police's handling of historical telecommunications data by the consultancy and audit house Deloitte.

The Danish Data Protection Agency's decision only concerns the National Police's own account of the case. Thus, reference will be made to Deloitte's investigation only to the extent that the comments in the statement give rise to it, and this decision has not - further - taken a position on the content and results of the independent investigation.

According to the Danish Data Protection Agency, the case concerns a number of errors, sources of error and uncertainties, etc. in teledata, in particular conversion errors in raw data (section 2.1), deficient raw data on communication using newer services (section 2.2) and incorrect conversion of mast coordinates (section 2.3).

In addition, it follows from the National Police's statement that there are a number of other errors, sources of error and uncertainties that may be relevant to the investigation. In this connection, special reference is made to sections 6.2.4 and 6.3 in the National Police's report. As these are minor errors and uncertainties that are not of the same magnitude as those mentioned above, these errors and uncertainties are assessed by the Danish Data Protection Agency not to have had an

impact on the data subjects' rights and freedoms, just as the Authority has noted that the sources of error mentioned mv. has been discussed with the Attorney General and informed to the police districts at the technician level. The Danish Data Protection Agency has therefore not found a basis for reviewing and taking further action in relation to these other errors, sources of error and uncertainties.

2.1. Conversion error in raw data

It appears from the National Police's statement that the National Police's Telecenter

Has since 1 November 2010 converted the raw data received from the telecommunications providers. Raw data is received in different formats from the telecommunications providers, and the telecentre's systems convert this information so that it appears to the requester in uniform formats and with uniform designations, regardless of which telecommunications providers have provided data (…). The conversion enables the case officer to compile and analyze data across the information obtained and subsequently for the prosecutor to present the information in a uniform manner during a possible criminal case. "[2]

Furthermore, it follows from the statement that three factors in particular have meant that not all raw data has been converted. It deals with an IT system error (section 2.1.1), errors in the handling of information about so-called special services (section 2.1.2) and an error in the provision of teledata via an analysis tool (section 2.1.3.). It also follows that other factors may have led to differences between raw data and converted data such as change in the formats in which raw data is delivered, or damaged or erroneous raw data in the form of unreadable characters, unintentional line breaks, etc.

2.1.1. IT system error

It appears from the National Police's statement that

”There was a systematic error in an IT system, which meant that in several cases differences were found between raw data and converted data. A major reason for these differences was an error in the IT system that the telecentre uses to convert teledata. The telecentre assesses that the error consisted of two elements; partly activation of a timer in the IT system, partly an update of the IT system. ”[3]

It also appears that the error was found in cases from 2012 until March 2019. The errors found in 2012 relate only to the timer.

Furthermore, it appears from the statement that

“The IT system, which the telecentre uses to convert teledata, has a built-in self-developed timer. The function of the timer has been to ensure that data was sent to the requester as soon as possible after data from the telecommunications provider had

been received in the telecentre's systems. The timer function has caused data to be sent in some cases, even though the overall conversion had not yet been completed, so that incomplete converted data sets were delivered to the requester. It was the intention that in such cases a complete data set should be sent subsequently, which, however, did not happen in all cases, cf. below. ”[4]

The National Police has further stated that

"An update of the IT system, which changed the way converted teledata was loaded into the system, has partly led to the loading becoming slower, and partly to the IT system skipping sections of files. This update is estimated by the telecentre to have taken place in May 2013. The slower data loading - in combination with the timer - is estimated to have meant that the IT system has increasingly delivered files with converted data to the requisitioners before all data has been included in the files. . In cases where an incompletely converted dataset has been provided, the system should - after the first unfinished delivery - have completed the conversion and forwarded a fully converted dataset to the requester. However, such automatic retransmission of teledata is not seen to have taken place in all cases, and the police districts have therefore in these cases not automatically received complete converted data sets.

The Telecentre has found that lack of converted teledata due to the update of the IT system and the timer occurs in different case types. These include on cases where the amount of data ordered has been so extensive that the converted data has not been able to be loaded in its entirety for delivery to the requester within the time for which the timer has been set. The error has also been seen in cases with amounts of data that could individually be handled within the time-limited capacity to which the system has been subject, but where in cases where the system has received many smaller files at the same time, a "queue" has occurred. in the system, whereby all converted data has not been loaded within the set time frame to which the timer has been set. ”[5]

It also follows from the statement that the update of the system has also had an impact on the handling of sections of files in connection with the loading of teledata. It thus appears that

In certain situations, it has been found that the loading of a file section was stopped before the entire file section was loaded. The Telecentre's investigations show that the system has not monitored such events, and therefore the loading of data from the relevant file section has not been resumed, and the loading of the file section has thus not been completed. Instead, the IT system began processing the next file section of teledata. Thus, there may be cases where the requester has not received all

the converted data. ”[6]

It is the National Police's assessment that the error was resolved on 8 March 2019. In addition, the telecommunications center has changed the method for how the system loads converted data and made adjustments in the system to ensure that the system can handle file sections. [7]

2.1.2. Error handling information about so-called special services

In addition to the above-mentioned errors, the National Police has uncovered that certain types of data - called special services - have not been converted for a period of time.

It appears from the National Police's statement that the telecentre - when converting teledata - uses the data type "other activity" as a term in the converted telecommunications information, which covers various special services such as call forwarding, "call-on" and number blocking. Information on activating and deactivating such special services has been provided by one telecommunications provider as part of teledata since 2010. [8]

In May 2018, however, the National Police became aware that information about special services was included in raw data, but not in converted teledata. The National Police assessed that the lack of conversion of special services was due to a change in the telecentre's IT system, which meant that the data type was sorted out in connection with the conversion, so that information only appeared on the raw data received by the requester. [9]

The National Police estimates that the error could have occurred in November 2016, when the system change was made. The error was corrected in June 2018. It is thus concluded that information about special services from one telecommunications provider is not included in converted data sets requested in the period from November 2016 to June 2018. [10]

2.1.3. Error in the delivery of teledata via analysis tool

The National Police has stated that

"Since January 2017, requisitioners with special user rights have been able to access converted teledata via a separate analysis tool in the telecentre's IT system, in which the converted information is entered and which can be used to process historical teledata." [11]

In August 2018, however, the National Police found that

"Information in converted teledata about the data types" other activity "and" services "(mainly SMS services in the form of eg SMS tickets, SMS donations, etc.) provided to the police by a telecommunications provider had not been loaded in the analysis

tool. In addition, the call center found that converted mast information was not loaded into the analysis tool in the case of datasets that only dealt with information about the mast locations of certain telephone numbers. The Telecentre's investigations have shown that entire sets of data with converted mast information from all four telecommunications providers have not been made available in the analysis tool. ”[12]

On the basis of the telecentre's own investigation, the National Police has identified almost 40 requisitions, where it cannot be ruled out that the requester has only worked with converted teledata via the analysis tool. [13]

2.2. Inadequate raw data on communication using newer services

Calls and SMS can be made through the use of newer call services (VoLTE and VoWiFi). Based on a specific investigation where information was missing in raw data, it was found in June 2019 that not all telecommunications providers have provided all information about these new data types.

It appears from the National Police's statement that

“The telecommunications provider that provided information in the case in question has, according to information, offered VoLTE and VoWiFi to its own customers since 1 August 2018, but had only provided information about these activities to the police from 10 January 2019. Against this background, in June 2019, the telecommunications center identified the cases where information from the telecommunications provider in question could be missing. New raw data were then sent to the police districts, etc. in those cases where there was a lack of information about these activities and where the police districts, etc. had not even previously requested new datasets. It has subsequently turned out that some of the activities in question were included in the original data sets that had been sent to the police districts, etc., but that the activities were not named correctly. "[14]

The telecommunications provider in question, together with the National Police, has reviewed raw data sets and has identified a further approx. 60 cases where information on the activities in question was missing.

It also appears from the statement that

”Another telecommunications provider around the turn of the month June / July 2019 [has] informed the telecentre that the provider from around April / May 2017 began rolling out VoLTE and Vo-WiFi activities to its subscribers. However, the provider has not logged information about these activities when it came to incoming calls to customers with a special business subscription. This information has thus not been included in raw data from April / May 2017 until mid-August 2019, when the

telecommunications provider has stated that it has corrected its registrations in order to ensure that information on VoLTE and VoWiFi activities is provided to the police. regardless of subscription type. ”[15]

2.3. Error converting mast coordinates

On the basis of an inquiry from the North Zealand Police on 25 July 2019, the National Police Telecenter stated that converted geographical coordinates for mast positions in a case from 2016 had been changed so that the masts 'location in the converted information did not match the masts' location in raw data. [16]

It appears from the statement that

“The error was that the mast coordinates were shifted approx. 222 meters in a south-southwest direction when the coordinates were compared with the raw data. It appeared i.a. of the information that this was not a deletion of raw data in the conversion, but that the conversion had caused a ‘distortion’ of data. At that time, the Telecentre assessed that the error was not critical, as it only concerned the location of the mast, the displacement was limited, and that data only showed which mast the telephone was on - and thus it was not an attempt to indicate exactly where the telephone was. . The Telecentre also assessed that the error could nevertheless be critical for more fundamental reasons. ”[17]

In the National Police's report, the Telecentre assesses that

“The errors found in the converted geographical coordinates for mast positions are due to errors in the IT systems in the telecommunications center that have translated the coordinates from the telecommunications provider's format to the format used by the police. In addition, the conversion error may be due to a lack of communication with telecommunications providers, which may have meant that there was no clarity about the format to be converted. ”[18]

The Telecentre also assesses that

“The error could have occurred in the period from September 2014, when a change was made to the system used, and until November 2016, when the telecentre had become aware of the error and made system adjustments to ensure a correct translation. The telecentre is not seen at that time to have informed the police districts etc. about the problem. ”[19]

In order to find the cases where there are errors in the converted mast coordinates, the telecentre in August 2019 conducted a review of the mast positions in all data sets that the telecentre had found at that time. Based on this, the telecentre has identified almost 350 data deliveries where the error occurs.

It follows from the National Police's statement that

“This is partly about almost 130 cases where the information was provided by a telecommunications provider in the period from the end of August 2016 to the end of October 2016, and partly about approx. 220 cases where the information was provided by another telecommunications provider in the period from around mid-March 2015 to mid-June 2016. In the converted data sets that the telecentre has examined, all the mast positions have been changed by a length of approx. 100 meters and up to approx. 220 meters in relation to the information in the raw data. The error was not found in data sets delivered in periods other than those mentioned above, including the period from September 2014 until June 2015. However, isolated examples have been found that a requester in 2012 and 2014, respectively, found a conversion error. It is not yet clear whether this is due to errors in the IT system or inadequate communication about the format with the provider. ”[20]

Furthermore, it appears from Deloitte's independent investigation of the National Police's handling of historical teledata that

”The analysis shows (…) that in the period 2011-2019 there have been shifts of mast coordinates in connection with the National Police Telecenter's conversion of mast positions. Specifically, 461 requisitions have been identified with incorrect conversion of coordinates on the starting mast and 385 requisitions with incorrect conversion of the final mast. The vast majority of these offsets are due to a conversion error, where mast coordinates are offset by approx. 222 meters. In addition, a small number of requisitions have been identified with shifts of mast coordinates of approx. 100 meters.

Deviations of this magnitude will in most cases not be significant in light of the general uncertainties associated with geographical location when using teledata. However, especially in denser urban settlements, where cells generally cover a smaller area, even minor displacements can potentially be significant in specific situations.

In addition, a limited number of requisitions have been identified with very large deviations. These deviations are considered to have a scope where it will be completely obvious to the users of historical teledata in police districts, etc., that there is an error. ”[21]

In addition, it follows from Deloitte's investigation that

“In relation to mast positions, it can be emphasized that the conversion errors found will in most cases not be significant in light of the general uncertainties associated with geographical location when using teledata. However, especially in denser urban areas, where cells generally cover a smaller area, even minor shifts can potentially be significant in specific situations. ”[22]

2.4. Deletion of teledata in the telecentre

It appears from the National Police's statement that

“Section 791 of the Administration of Justice Act lays down rules on the deletion of material which has been obtained by interfering with the secrecy of communications. Teledata obtained in accordance with the Administration of Justice Act, section 780, subsection 1, nos. 3 and 4, are covered by these rules. Pursuant to the Administration of Justice Act, section 791, subsection 1, the material must be destroyed if no charges are brought against anyone or if charges are later dropped. However, the court may, pursuant to section 791, subsection 2, provide that destruction may be omitted or postponed. Pursuant to section 791, subsection 4, the police must otherwise destroy material which is obtained by interfering with the secrecy of communications and which proves to be of no investigative significance. "[23]

It also appears that the Public Prosecutor's Office has clarified that it is the individual police district that must ensure that the material is deleted in accordance with applicable law. Deletion must take place by the police district submitting a deletion requisition to the National Police, at the same time as the police district ensures that any copies of the material stored locally in the district are also deleted.

In addition, it follows from the statement that

“Especially for the telecentre, it is noted that teledata is stored in the telecentre after the end of the data processing. The raw data stored must be deleted if the requester so requests. As far as converted teledata is concerned, the telecentre - when a data processing is completed - is in possession of two copies of the converted teledata. For capacity reasons, the telecentre has established a business process whereby this telecommunications data should be deleted automatically, unless the requester who requested information before the expiry of this period has notified the telecentre that the deletion must be postponed. The deletion of one copy of the converted data sets must take place after one year and the other copy must be deleted after another year. However, in mid-September 2019 in connection with the telecommunications case, the Telecentre found that the deletion of converted telecommunications data after two years has not taken place in full, and that approx. 75 pct. of these data sets in the telecentre. The automatic deletion of copies of converted teledata after one year is seen to have taken place. ”[24]

It is further stated in Deloitte's investigation of the National Police's handling of historical teledata that

"There has not been a consistent practice in relation to the National Police's Telecenter's deletion of the database version, which is why copies of it are still available in a number of cases where the requisition took place more than 24 months ago." [25]

2.5. The National Police's technical and organizational measures

It appears from the National Police's statement that

In the period from the end of June to 25 September 2019, the National Police's Unit for Supervision and Control (hereinafter ToC) investigated the telecentre's handling and processing of teledata with special focus on process and workflows, quality assurance activities and controls, collection of identified errors and managerial orientation and handling. of identified defects. ”[26]

ToC is the police's internal control and supervisory unit, which can, upon request or on its own initiative, initiate investigations into all aspects of the police's activities. To ensure the unit's independence, the unit reports directly to the National Police's Executive Board. The concrete investigation of the telecentre was initiated in the days following a meeting with the National Police Chief on 19 June 2019. [27]

2.5.1. Quality control

ToC has found that the existing controls in the telecentre have to a lesser extent focused on validating the quality of data, which i.a. is supported by the fact that controls have been established, which carry out technical validation of the file before it is subsequently converted, and which ensures that data is actually sent to the requester. [28]

Furthermore, ToC has found that there appear to be differences in the police districts' control of quality assurance of teledata from the telecentre. In an investigation carried out by the National Police's Police Area, individual districts have thus stated that when receiving teledata, they have separate workflows to ensure control of and quality assurance of obtained teledata. One police district has stated that the reason why the district has not had separate checks on telecommunications information obtained is that they have not had reason to question the validity of telecommunications information received from the telecommunications center before the information about the now identified errors in telecommunications data.

Deloitte's investigation of the National Police's handling of historical teledata also shows that

"In general, no quality assurance has been carried out on historical teledata in the police districts, etc., including no completeness check of received historical teledata before the turn of the year 2018/2019." [29]

2.5.2. Education and competencies

It appears from the National Police's report that the police district investigators acquire competencies in relation to teledata for use in investigations in either peer training or in courses on teledata. These courses are generally not aimed at investigators,

and have only been offered at the beginning of 2018, which is why a large part of the investigators' competence building is based on peer training, which may mean that police district investigators do not necessarily have the competencies to control quality. of the data sets received. It is noted in this context that the Public Prosecutor's Office annually offers a course targeted at prosecutors regarding the use of teledata in court. [30]

In Deloitte's investigation of the National Police's handling of teledata, it is stated that the investigators' competencies vary in the police districts:

“In general, investigators are trained in the use of historical teledata by peer training of more experienced investigators, but there is no actual training plan or course for new investigators. Courses in the use of historical teledata have previously been offered in some police districts, but the courses are not held consistently and have varying content. Courses are not offered and only to a limited extent guidance from the National Police Telecenter. This means that there is a risk that investigators are not aware of the uncertainties associated with the use of historical teledata and thus misinterpret data. ”[31]

2.5.3. Collection on errors

It follows from ToC's investigation that during the investigation period there was no fixed practice or procedure in the telecentre to record or document reported errors and the associated description of any error solution in a central system or document. In this connection, the National Police Telecenter has stated that it is possible to report errors in received data in at least five different ways.

It is on i.a. the background ToC’s finding that

"For most of the investigation period, the Telecentre has not had a fixed practice or procedure for noting and documenting reported errors in a central system or document where a possible error solution could also be described." [32]

Furthermore, it appears from Deloitte's investigation of the National Police's handling of historical teledata that

"Police districts, etc. has not established unambiguous communication channels in the event of a need for support or for reporting identified errors regarding the use of historical teledata. Apart from an annual ERFA group meeting, with the participation of teledata analysts and other designated knowledge persons, no forums for ongoing knowledge sharing have been established. A forum for teledata analysts for knowledge sharing has been set up in 2018, but there is limited knowledge of this forum in the circles. ”[33]

The Telecentre has stated that for a 2-year period in the years between 2011-2014, they have used the HP service manager

for error handling processes.

It also appears from the National Police's report and ToC's investigation that in cases where a problem has been reported with a data set from a requester, this has often been solved by having the file in question been reviewed and the telecentre then made a re-run. of the request. The applicant has then received the data set again. As an example, error messages regarding conversion errors have basically been solved by the telecentre troubleshooting the problem, if possible correcting the specific error, reconverting data and retransmitting data to the requester. [34]

It is against that background that ToC's finding that

"The employees in the telecentre have thus continuously solved the requisitioners' problems with data throughout the investigation period. At the same time, these have been resolved as soon as possible, so that the ongoing investigation is not delayed unnecessarily.

The method of solving the problem has been individual and is not documented.

At the same time, the Telecentre has stated that if a problem has occurred several times, the employees have tried to find a solution that could prevent the problem from occurring in the future. However, there has to a lesser extent been a common reflection on the errors found, and this has contributed to errors being resolved without it being investigated why errors occurred again and again. "[35]

Regarding any managerial orientation and handling of potential and identified errors, etc. ToC states, in the National Police's statement, that

"Searches in minutes from executive board meetings, group management meetings, senior management meetings and extended senior management meetings in the Police Area as well as minutes from the forum for chief police inspectors in the police have not found information showing that potential and identified errors in teledata have been submitted and discussed at the said meetings during the IP. "[36]

It has only been possible to find individual examples from 2012 and 2015.

It appears from the statement that ToC has not

Found evidence that the error in relation to discrepancy in the number of activities between raw data and converted data has been managed managerially at a level above the telecentre's management before November 2018. The investigation also shows that knowledge that it was a systematic error in connection with the conversion, will first be known in the top

management of the Police Area at the beginning of 2019. ”

However, already in September 2018, on the basis of a circuit inquiry, the telecommunications center identified errors and issues concerning the discrepancy between received raw data and converted data. The then head of the telecentre was informed about this. "[37]

2.6. The National Police's responsibility and documentation of quality control

ToC has found that during the investigation period, there have been no written guidelines, guidelines or procedures for internal use in the telecentre in relation to the handling of teledata.

It follows from the statement that

“During the study period, no national guidelines have been drawn up for how the police districts should handle and ensure the quality of data received from the telecentre. The telecentre sends a technical guide to the requester together with the transmission of data. The guide contains i.a. information about what data the received files contain and how the files are opened and subsequently loaded. The technical guide is not dated, so it is not clear when the guide was valid from.

The most recently updated technical guide was adopted in December 2018. The updated guide states as something new that the requester must always check whether the number of activities in the raw data is in accordance with the converted data.

Some police districts have prepared local guidelines for their processing of telecommunications information. The local guidelines focus primarily on determining and clarifying the procedure for interfering with the secrecy of communications and the destruction of material from interference with the secrecy of communications.

It is stated that in NC3 since 2017 there has been a general focus on increasing the degree of writing and documentation. However, the Telecentre has stated that they have not experienced that this focus has been directed towards the Telecentre's work. ”

ToC has further found that during the period there have been no system descriptions of the IT systems and databases used in the telecentre in connection with the handling of teledata. [38]

Deloitte's independent investigation of the National Police's handling of historical teledata shows that

"Especially processes for quality control to a very limited extent have been documented" [39]

And furthermore, that

"The post-processing, analysis, adaptation and enrichment of other data lists carried out by teledata analysts and investigators

are generally not logged or recorded, making it difficult to follow the transaction trace." [40]

In addition, it follows from the National Police's statement that

“In 2011, the telecentre prepared a flow description for the telecentre's self-developed IT solution, which collects data from the supplier and sends the ordered data to the requester. The in-house developed solution has been further developed since 2011, but without an associated update of the flow description.

No requirements specification was prepared for the solution when the telecentre in January 2015 began the development of a new in-house developed platform for the conversion of teledata, which was completed in November 2016. It is therefore unclear from the available information what the need was and whether it developed solution met the need.

The National Police has initiated work to develop a new and more up-to-date system for converting and storing teledata. No project initiation document, business case, requirements specification or the like has been prepared, which is otherwise the starting point for the National Police in the development or adaptation of already existing IT systems. ”[41]

2.7. Summary of ToC’s study

In summary, ToC concludes that:

the telecentre has sought to solve the problems concerning received teledata in relation to the individual case as soon as possible. The issues are often resolved as a single technical and operational matter.

there have been no written internal procedures, guidelines or guidelines for internal use in the telecentre in relation to the handling of teledata. Similarly, no national guidelines have been drawn up for the circuits' handling and quality assurance of teledata.

the telecentre's controls of teledata have primarily aimed at providing data to the users in the police districts as soon as possible rather than being input and output controls to ensure the quality of the content of received and processed teledata.

for large parts of the investigation period, there has been no structured collection, documentation and follow-up of reported errors. Lack of systematics and documentation in the general error solution has made it difficult for the telecentre to categorize the individual errors and prioritize the subsequent error solution as well as to organize the information about errors.

measures to inform users of teledata in the circles about e.g. found errors and inconveniences have occurred but have not been sufficiently adequate and stringent. Police districts have not been systematically and completely informed about the possible errors and omissions in data that they should be aware of when using teledata.

the errors now identified show that the procedures, methods and systems used in NC3 and the police districts, overall, have not been suitable for ensuring the quality of teledata.

there does not seem to have been the necessary managerial focus on ensuring the employees a sufficient framework and opportunities to solve their tasks with the necessary quality.

the telecentre in September 2018 - in collaboration with NEC identified errors and issues - regarding discrepancies between received raw data and converted data, which indicated systematic errors in connection with sending data to the police districts.

it does not indicate that the error regarding discrepancies in the number of activities between raw data and converted data has been dealt with managerially outside the telecentre before November 2018. The study also shows that knowledge that there was a systematic error in connection with the conversion, first becomes known in senior management in the Police Area in early 2019.

There have been ongoing inquiries about errors and deficiencies in data, including inquiries in both 2012 and 2015. There has thus been a need for and specific opportunities for management to focus on the area outside the telecommunications center as well. [42]

In conclusion, ToC concludes that

“Teledata is characterized by data that has been collected for the use of the telecommunications providers' activities, but which can be used to advantage in the work of the police and the prosecution. In summary, it is ToC's assessment that this has not been sufficiently taken into account in the processing of teledata during the investigation period. Thus, there have been insufficient processes, workflows and quality assurance activities in the telecentre to ensure the quality of the delivered teledata, just as there has been inadequate communication to the districts and further in the criminal case chain about known shortcomings in the content of data. This, combined with the districts' inconsistent practice of quality control of data and an apparent lack of managerial focus in the field, has meant that the best possible quality of teledata has not always been provided. "[43]

2.8. Number of cases

It follows from the National Police's statement that

“On 22 March 2019, there was a revised draft of the memorandum of 17 March 2019, where, among other things, It appeared that the telecentre's investigations had shown that in the period from the beginning of 2012 to the beginning of March 2019,

there could be cases where the police districts had received incomplete teledata sets from the National Police. Regarding the scope of the problem, it appeared from the memorandum that the telecentre had identified approx. 600 cases in 2017 and 2018, where the police districts had received data sets where the number of rows of activities in converted data did not match the number of rows of activities in the corresponding set of raw data. A further review of the telecentre's archive for teledata indicated, according to the memo, that in the years from 2012 to 2015, there were on average at least 150 cases a year with insufficiently converted data. However, the telecentre's assessment was that the divergence for the years 2012-2015 did not really cover a difference between activities in raw data and converted data, as the majority of the identified cases covered a compilation error in one row, and that this was a known data compilation challenge. The memorandum concluded that the errors in a very large proportion of the identified cases concerned special services and that the conversion of special services could have been incomplete in the period from November 2016 to June 2018. ”[44]

It also follows from the National Police's statement that the analysis of possible conversion errors before 2013 showed that ”Which in 19 out of approx. 900 requisitions examined from 2012 were signs of errors in the conversion. Of the 19 requisitions, it was the telecentre's assessment that 4-5 of these were due to the timer in the IT system. ”[45]

In its investigation of the National Police's handling of historical teledata, Deloitte has essentially confirmed the results that the National Police's internal investigations and random checks have uncovered. It thus appears i.a. of the study that

“The analysis of the National Police's conversion of historical teledata at row level shows overall that there have been discrepancies in the number of rows between converted data and raw data for approx. 6.9 pct. that they examined requisitions. Of these, there are row losses (ie fewer rows in converted data than in the raw data file) in 1,131 requisitions in the study period corresponding to approx. 5.8 pct. of the requisitions. This corresponds to DKK 4.5 million. lost rows. The study shows that the row loss is predominantly concentrated in 2016, where 361 requisitions with row losses have been identified. The extent of row losses is also highlighted. 142 requisitions with a divergence of one row have been identified, 260 requisitions missing 2-10 rows, 275 requisitions missing 11-100 rows and 453 requisitions missing more than 100 rows in relation to converted data. The extent of row losses must be seen in the light of the number of rows in a requisition, where the average number of rows for comparison is approx. 3,900 rows, while the median is approx. 400 rows. Overall, Deloitte identifies a smaller percentage loss of range than what the National Police has identified in its internal screening of 2018. ”[46]

461 and 385 requisitions have been identified with discrepancies in the conversion of the mast coordinates for resp. start and

end mast. [47] The vast majority of these offsets are due to a conversion error, where mast coordinates are offset by approx. 222 meters. In addition, a small number of requisitions have been identified with shifts of mast coordinates of approx. 100 meters. Finally, a very limited number of requisitions have been identified with very significant displacements of mast positions. [48]

2.9. The National Police's work with and knowledge of errors, sources of error and uncertainties in teledata

It follows from the National Police's statement that it is not unknown to the authority that errors, sources of error or uncertainties may occur in teledata used during criminal proceedings.

It appears from the statement that

“As mentioned in the Ministry of Justice's answer of 20 October 2015 to question no. 182 (General Part) from the Parliament's Legal Committee, it has, among other things, It has been known that the National Police has previously in some cases found that the telecommunications providers 'mast lists have not been correct and continuously updated, that there have been errors in the telecommunications providers' historical lists of mast locations, and that there has been no accurate registration of the transmission cells. mobile phone has used in connection with data traffic. "

And furthermore, that

“As is also apparent from the answer of 20 October 2015 to question no. 182 (General Part) from the Parliamentary Legal Affairs Committee, there have previously been specific cases where inaccurate mast information has been included. For example, in a specific case, errors were discovered in connection with the preparation of a mast card, as the mast positions in the telecommunications information received from the telecommunications provider were so volatile within very short time intervals that it would not have been physically possible to move so quickly between the masts. .

As stated in the same answer, it has also been known that there can be different physical conditions, which means that a mobile phone e.g. jumps to another mast, cf. also the Public Prosecutor's Office's external guidance on the presentation of telecommunications information referred to in section 4.2.2 of the [statement]. ”

In addition, it appears from the report that the telecommunications center has continuously handled inquiries about possible errors, inaccuracies, sources of error, etc. in teledata received by the requesters from the telecentre. These inquiries have mainly been handled by re-processing the relevant teledata in the telecentre and were perceived by the National Police primarily as user errors and periodic technical challenges rather than systematic errors regarding teledata. [49]

It thus appears from the statement that

Thus, for example, in February, May, August and September 2018, the Telecentre received inquiries from requisitioners who found a lack of historical telecommunications information in converted data sets, which was handled in the specific cases, but without giving rise to a more systematic review of data. In cases where the error reports have dealt with incomplete information in the raw data, the telecommunications center has most often dealt with it by communicating with the relevant telecommunications provider about the specific missing information and thus not treating it as a possible systematic error. The inquiries have reportedly been handled by employees in the telecentre with the alternating involvement of the then heads of the telecentre. ”

As an example of the National Police handling issues concerning teledata at a higher management level, reference is made in the report to a meeting in 2012 between e.g. the then police director for the police area and a telecommunications company. [50]

It also appears from the statement that the National Police, on the basis of a specific ongoing investigation, in November 2018 suspected that there could be a general conversion error in the IT program in the telecentre, which converted raw data and passed this data to the relevant requester . In the specific case, immediately unexplained discrepancies were found between raw data and converted data, so that parts of the raw data were not included in the converted data, which was conveyed from the telecentre to the police district. The then head of the area and of the National Police's Cyber Crime Center (NC3) was informed in mid-November 2018 about the missing telecommunications information in the specific case. [51]

On the basis of the inquiry, the telecentre conducted a random sample in November 2018 with a view to clarifying whether there were any immediate signs of a general error.

It appears from the statement that

The random check included 60 randomly selected cases - 30 from 2017 and 30 from 2018. The check - which is not documented and thus not possible to recreate - allegedly showed that the vast majority of the checked cases were correctly converted, while in a few cases there was a difference between raw data and converted data with up to four lines difference in the respective spreadsheets. ”

The National Police Telecenter assessed, on the basis of the inspection, that

"The differences shown by the sample did not indicate a general system error, and that the conversion error in the specific

case was due to the large data files obtained for the case in question, which were very large."

On the basis of the above, on 28 November 2018, the Telecentre inserted a new section in the instructions that were provided to the requester together with the files with raw data and converted data. In the new section, it was stated that before using converted data, the requester should always make sure that the number of rows of activities in the two data sets was consistent. However, the applicants were not made specifically aware of this change. [52]

2.10. The National Police's measures taken

It follows from the National Police's statement that the National Police and the Public Prosecutor's Office have initiated the following measures to counter the errors found:

Modification of the instructions provided to the requester, together with raw data and converted teledata, to make the requester aware of the completeness of the converted data. [53]

Introduction of an automatic counting control, which aims to ensure that in the individual requisitions there is a correspondence between the number of rows of data in raw data and converted data. [54]

In addition to the manual control in the police districts, etc. has the telecentre introduced a systematic manual control of the data sets delivered to the police districts, etc. It is checked whether the number of rows in the respective data sets matches. If it is found that information is missing, the police district, etc. contacted as soon as possible. [55]

By the instructions of 2 July 2019, the Public Prosecutor's Office instructed all prosecutors that in connection with the processing of criminal cases involving telecommunications information, considerable caution should generally be exercised in attributing the lack of telecommunications information to the significance that there has been no telecommunications or the like. [56]

Subsequently, on 18 August 2019, the Attorney General issued an instruction to the country's prosecutors that prosecutors may not use telecommunications data, including signaling data and telecommunications observation, during main hearings or court hearings regarding the maintenance of arrest. The letter stated that the temporary suspension would be valid for 2 months until further notice. [57]

With regard to the use of teledata during other parts of the investigation than as a basis for custody, the National Police has by letter of 30 August 2019 to the police districts, etc. and in the instructions of 18 September 2019 laid down guidelines for the police's use of teledata during the investigation. It instructs caseworkers to pay special attention to the review, control and use

of teledata, including paying particular attention to the errors, sources of error and uncertainties that have been identified so far. At court hearings during the investigation, where a request for coercive intervention is made, requests must in future be based on raw data. The Public Prosecutor's Office also issued an instruction of 30 August 2019 with reference to the National Police's guidelines of the same date, in which all prosecutors were similarly instructed that requests for coercive intervention during the investigation must be based on raw data. [58]

In continuation of the above measures, the National Police launched an external investigation on 27 August 2019 to create sufficient clarity as soon as possible about the errors, sources of error and uncertainties associated with the use of teledata, so that teledata can again be used as evidence in criminal cases. [59]

In addition to the above-mentioned measures, the National Police has sent a copy of the National Police Chief's and the Attorney General's considerations and new initiatives on the basis of the teledata case.

Justification for the Danish Data Protection Agency's decision

Everyone has the right to data protection and anyone who processes personal data is obliged to respect the rights of data subjects and to protect personal data.

It follows from Article 6 (1) of the European Convention on Human Rights. 1, at

Everyone has the right to a fair and public hearing within a reasonable period of time before an independent and impartial tribunal established by law, whether in a dispute over his civil rights or obligations or in an indictment against him. crime.

The case thus concerns a basic human right, and it is fundamental for the Danish Data Protection Agency that everyone, including the actors in the case, but also the outside world, can trust the information that the police process and pass on to police districts and ultimately the information presented by the prosecution. The Danish Data Protection Agency assesses that lack of data protection in the criminal case chain in particular - in addition to loss of rights for the data subjects - can lead to weakened confidence in both the police and the courts.

The Danish Data Protection Agency is of the opinion that the processing of information worthy of protection and the context in which the information is included entails a high risk for the rights and freedoms of the citizens concerned, as the processing of incorrect or incomplete information may involve serious violations of citizens' rights. to a fair trial, interference with personal liberty, as well as general privacy matters.

As this case concerns a fundamental human right, the Authority considers the case to be an unacceptable example of the

potential realization of some of the most serious risks to data subjects which the lack of data protection may entail.

3.1. Treatment safety

According to the Law Enforcement Act, section 27, subsection 1, the controller and the processor - taking into account the current technical level, the implementation costs and the nature, scope, context and purpose of the processing and the varying probability and seriousness of the risks to the rights of natural persons - shall implement appropriate technical and organizational measures to ensure a level of security appropriate to these risks, in particular as regards the processing of the special categories of personal data covered by section 10.

Thus, as part of the implementation of appropriate technical or organizational measures, the data controller must assess the risks involved in a processing and implement measures that can limit these risks. In general, the need for protection will increase the more sensitive personal data is processed. The data controller must therefore consider the need for protection of the information being processed.

Considering that the processing of personal data in the form of teledata for the purpose of prosecution is likely to involve a high risk of data subjects' rights and freedoms, the Danish Data Protection Agency considers that there must be a high level of data protection, in particular that the data is correct and true and fair.

Based on the information provided, the Danish Data Protection Agency primarily assumes that the National Police has acknowledged that, in general, no quality assurance has been carried out of historical telecommunications data or completeness checks of received historical telecommunications data from the National Police Telecenter. The National Police has also acknowledged that the telecentre's controls have to a lesser extent focused on validating the quality of data, that there is a difference in the police districts' control of quality assurance of teledata from the telecentre, and that the processes for quality control have been documented to a very limited extent.

Furthermore, the Danish Data Protection Agency assumes that there has not been sufficient education and training of the employees in handling teledata and data protection, including processing security. In this connection, the Danish Data Protection Agency has - according to what the National Police stated in the report - assumed that the competence building of the police investigators is based almost exclusively on peer training, and that there is no real training plan or course for new investigators.

The Danish Data Protection Agency also assumes that the National Police Telecenter has not had a fixed practice or

procedure for noting or documenting reported errors and the associated description of any error solution in a central system or document. In this connection, the Danish Data Protection Agency attaches importance to the National Police's information that it is possible to report errors in received data in at least five different ways.

In addition, the Danish Data Protection Agency assumes that any errors for years - the first errors were found in 2012 - have been resolved on an ad hoc basis, as soon as possible, individually and undocumented. It appears from the case that in February, May, August and September 2018, the National Police Telecenter received inquiries from requisitioners who found a lack of historical telecommunications information in converted data sets, which was handled in the specific cases, but without giving rise to a more systematic review. of data. The Danish Data Protection Agency has further emphasized that it appears from the National Police's own statement that there has been a lesser joint reflection on established errors, which has contributed to errors being resolved without it being investigated why errors occurred again and again.

The Danish Data Protection Agency also assumes that the National Police - in addition to a few examples from 2012 and 2015 - has not found information showing that potential and identified errors in teledata have been submitted and discussed at executive board meetings, group management meetings, senior management meetings, extended senior management meetings leadership in the Police Area or in the forum for chief police inspectors in the police. The Danish Data Protection Agency has further assumed that despite errors in teledata since 2011, errors and issues concerning discrepancies between received raw data and converted data - in addition to a meeting in 2012 between e.g. the then police director for the police area and a telecommunications company - was only dealt with at a certain managerial level in September 2018.

The Danish Data Protection Agency also assumes that it follows from the National Police's statement that it is not unknown to the authority itself that errors, sources of error or uncertainties may occur in teledata used in criminal cases. It follows from i.a. response to the Parliament's Legal Committee that it has been known back in 2015 that the telecommunications providers 'mast lists have not been correct and continuously updated, that there have been errors in the telecommunications providers' historical lists of mast locations, and that there has been no accurate registration of the transmission cells. which a mobile phone has used in connection with data traffic.

In addition, the Danish Data Protection Agency assumes that the National Police, on the basis of a specific ongoing investigation, in November 2018 suspected that there could be a general conversion error in the IT program in the telecentre, which converted raw data and passed this data on to the relevant requester. . As there were discrepancies between raw data

and converted data, so that parts of the raw data were not included in the converted data, which was communicated from the telecentre to the police district, the telecentre conducted a sample in November 2018 to clarify whether there were immediate signs of a general error. The control is not documented and can not be restored, but showed according to what was stated in the statement that the vast majority of the sample-checked cases were correctly converted, which is why the National Police assessed that there was no general system error and that the conversion error in the specific case was due to large data files obtained for the case in question, which were of a very large size.

In this connection, the Danish Data Protection Agency assumes that the telecommunications center - on the basis of the incident - inserted a new section in the instructions that were provided to the requester together with the files with raw data and converted data. In the new section, it was stated that before using converted data, the requester should always make sure that the number of rows of activities in the two data sets was consistent. However, the applicants were not made specifically aware of this change. [60]

The Danish Data Protection Agency also assumes that the incorrect conversion of raw data - according to the National Police's own information - i.a. was due to the fact that the telecentre's IT systems did not monitor events where the loading of a file section was stopped before the entire section was loaded, and that the system's timer function has caused data to be sent in some cases, even though the overall conversion was not yet completed so that incomplete converted datasets were delivered to the requester. In this connection, the Danish Data Protection Agency has assumed that the system - after the first unfinished delivery - should have completed the conversion and sent a fully converted data set to the requester, which is why the Authority considers that the National Police has not taken sufficient technical measures to ensure an appropriate level of security.

In addition, the Danish Data Protection Agency assumes that an update of the IT system in 2013 was one of the reasons why there was a conversion error of raw data.

The Danish Data Protection Agency finally assumes that the telecommunications center became aware of the error in November 2016, and that the center made a number of system adjustments on that occasion. The Telecentre, on the other hand, did not inform the local police districts about the problem.

In the opinion of the Danish Data Protection Agency, the National Police has thus not sufficiently taken appropriate technical and organizational security measures to ensure an adequate level of security that suits the risks involved in the authority's

processing of personal data, including ensuring that the National Police does not process and pass on incorrect personal data in the form of incorrect or incomplete teledata.

In this connection, the Danish Data Protection Agency is of the opinion that all probable error scenarios should be tested in connection with the development of new software, where personal data is processed, and that testing and ongoing follow-up of any changes in the data controller's systems should be ensured. personal data is treated with lasting confidentiality, integrity, availability and robustness. In this connection, the Danish Data Protection Agency finds it aggravating that the information forms the basis for decisions regarding investigation, prosecution and prosecution, and that the information is used as evidence in criminal cases.

The Danish Data Protection Agency also emphasizes that this case, including the errors now identified, is an expression of several different types of errors and with varying causes. The Danish Data Protection Agency finds that the case is an expression of the fact that the procedures, methods and systems that have been used in the National Police Telecenter and the police districts in connection with the processing of teledata have overall not been suitable for ensuring the quality of the information or that employees have not been sufficiently aware of this.

In addition, the Data Inspectorate more generally assumes that the processing of the information has been going on for a number of years, that the processing relates to a large number of cases, that the National Police processes information worthy of protection about a very large number of citizens, and the context in which the information is included. can be used in connection with the police investigation and a possible later criminal case, which is why the Authority finds that the present processing of personal data entails a high risk for the rights and freedoms of the persons concerned.

On that basis, the Danish Data Protection Agency finds that the National Police's processing of personal data has not taken place in accordance with section 27 of the Law Enforcement Act.

The Danish Data Protection Agency has noted that, as a follow-up to this case, the National Police has taken a number of organizational and technical measures (section 2.10 above) and made a number of considerations and new initiatives.

3.2. Basic principles when processing personal data

3.2.1. § 4 pieces. 4 on ‘correctness’ and § 4, para. 5 on the quality of information on disclosure

It follows from the Law Enforcement Act § 4, paragraph. 4, that information that is processed must be correct and, if necessary, updated. Every reasonable step must be taken to ensure that personal data which are inaccurate in relation to the purposes for

which they are processed are deleted or rectified immediately.

Furthermore, it follows from § 4, para. 5, that the data controller takes all reasonable measures to ensure that personal data are not passed on or made available if they are incorrect, incomplete or out of date. To this end, the data controller verifies, as far as possible, the quality of the personal data before passing them on or making them available. In the context of the transfer of information, the necessary information shall be added as far as possible to enable the receiving competent authority to assess the extent to which the personal data are accurate, complete and reliable and the extent to which they are up to date. If it is found that incorrect personal data has been passed on or that personal data has been passed on illegally, this must be notified to the recipient immediately. The information must be corrected or deleted, or the processing must be restricted.

The National Police have acknowledged that they have provided incomplete data sets, processed incomplete raw data on communication using newer services and incorrectly converted mast coordinates. On this basis, the Danish Data Protection Agency finds that the authority has processed and passed on incorrect, incomplete and out-of-date personal data. On this basis, the Danish Data Protection Agency finds that the National Police has not complied with section 4 (1) of the Law Enforcement Act. 4 and para. 5.

The Danish Data Protection Agency assumes that in a number of cases the National Police has not entered information in converted teledata about the data types "other activity and" services "in the analysis tool, and converted mast information in the case of data sets that only concerned information about certain telephone numbers' mast locations. why it can not be ruled out that the requester has only worked with converted teledata via the analysis tool.

Furthermore, on the basis of the National Police's report, the Danish Data Protection Agency assumes that - due to a change in the telecentre's IT system in November 2016 - there are cases where information about special services was included in raw data, but not in converted teledata.

In addition, the Danish Data Protection Agency assumes that the National Police in 2019 has established that not all telecommunications providers have provided and are providing all information on new data types, including newer call services such as VoLTE and VoWiFi, which is why the National Police has identified a number of cases where information on newer call services. In this connection, the Danish Data Protection Agency assumes that one telecommunications provider has not logged information about these activities when it came to incoming calls to customers with a special business subscription, which is why this information has not been included in raw data from April / May 2017 until the middle of August 2019, where

the telecommunications provider has stated that it has corrected its registrations in order to ensure that information on VoLTE and VoWiFi activities is provided to the police regardless of subscription type.

The Danish Data Protection Agency also assumes that in the period 2011 to 2019 there have been shifts of mast coordinates in connection with the National Police Telecenter's conversion of mast positions, whereby the National Police has processed and passed on information about telemasters' location, where the converted geographical coordinates for mast positions were changed. the position of the masts in the converted information did not match the position of the masts in the raw data.

In this connection, the Danish Data Protection Agency also assumes that the vast majority of these cases consist of errors where the mast coordinates are shifted approx. 222 meters in a south-southwest direction, and that the incorrect coordinates were due to errors in the IT systems in the telecentre that have translated the coordinates from the telecommunications provider's format to the format used by the police.

The Danish Data Protection Agency also assumes that it cannot be ruled out that such a shift - for example in the case of denser urban settlements - can potentially have a significance and thus a risk to the data subjects' rights and freedoms.

In addition, the Danish Data Protection Agency assumes that the Danish National Police carries out non-negligible processing of personal data about a very large number of citizens, which in the Danish Data Protection Agency's opinion means that the Danish National Police should ensure the quality of the data stored and passed on.

The Danish Data Protection Agency also assumes that the processing of incorrect, incomplete and out-of-date information has been going on for a number of years, that the National Police has for years been aware that errors, sources of error or uncertainties may occur in teledata used in criminal cases. , that the processing relates to a larger number of cases and finally the context in which the information is included, including ultimately as part of a criminal case.

On this basis, the Danish Data Protection Agency finds that the National Police's processing of personal data has not taken place in accordance with section 4 (1) of the Law Enforcement Act. 4 and para. 5.

In this connection, the Danish Data Protection Agency must note that it is generally the principle that erroneous or incorrect information passed on to other data controllers must be rectified by informing the recipient of the information about the errors in question, cf. section 4 (1) of the Law Enforcement Act. 5.

On that basis, the Danish Data Protection Agency must recommend that the National Police assess this, and if necessary contact the recipients responsible for the data, unless they have been advised otherwise. Such notification shall contain

information that ensures that the incorrect information is corrected, or deleted, or that future processing is restricted.

The Danish Data Protection Agency must refer to the Authority's guidelines on data subjects' rights. [61]

3.2.2. § 4 pieces. 6 on storage limitation

It follows from the Law Enforcement Act § 4, paragraph. 6, that collected information may not be stored in a way that makes it possible to identify the data subject for a longer period of time than is necessary for the purposes for which the information is processed.

The Danish Data Protection Agency has reviewed the National Police's report. In this connection, the National Police has stated that when a data processing is completed, the telecentre is in possession of two copies of the converted teledata. One copy of the converted data sets should be automatically deleted after one year and the other should be deleted after another year. The National Police has further stated that according to the Administration of Justice Act § 791, para. 4 follows that the police must destroy material which is obtained by interfering with the secrecy of communications and which turns out not to be of investigative significance.

It is not the responsibility of the Danish Data Protection Agency to decide when the information in question is of investigative significance, and in this connection when a criminal step is necessary.

On that basis, the Danish Data Protection Agency finds no basis for overriding the National Police's assessment that personal data in the form of teledata is necessary to store for up to two years. In this connection, the Danish Data Protection Agency has assumed that the storage of teledata is regulated in the Administration of Justice Act, and that the National Police is seen to have taken a concrete position on how long the information needs to be stored.

However, the Danish Data Protection Agency assumes that the National Police has admitted to having stored approx. 75 pct. of the data sets in question in the telecentre and do not perform the automatic deletion of copies of converted teledata. On that basis, the Danish Data Protection Agency finds that the authority has not acted in accordance with section 4 (1) of the Law Enforcement Act. 6.

In this connection, the Danish Data Protection Agency assumes that the National Police Telecenter stores teledata after completion of the data processing, that the telecentre has established a business process, according to which one copy of this teledata should be deleted automatically after one year and another year for the other copy. There has not been a consistent practice in relation to the National Police Telecenter's deletion of the database version, which is why copies of the data sets

are still available in a number of cases where the requisition took place more than 24 months ago.

On that basis, the Danish Data Protection Agency finds that the National Police's processing of personal data has not taken place in accordance with the Law Enforcement Act, section 4, subsection. 6.

The Danish Data Protection Agency also finds grounds for issuing an order to the National Police to delete the personal data that meet the requirements for deletion in accordance with the telecommunications centre's own guidelines, the extent to which deletion has not already taken place.

The order is issued pursuant to section 42 (1) of the Law Enforcement Act. 1.

The deadline for compliance with the order is 6 weeks from today's date. The Danish Data Protection Agency must request receipt of a confirmation that the National Police has sufficiently deleted the personal data in question.

In addition, the Danish Data Protection Agency must recommend to the National Police that guidelines be prepared for deletions that are complied with, checked and sanctioned. This also applies to the data sets that have been passed on to requisitioners, and routines must be incorporated that ensure that all representations of data, at all stages of the organization, are deleted.

3.3 § 4, para. 8, cf. § 4, para. 7 on "responsibility"

It follows from the Law Enforcement Act § 4, paragraph. 8, that a data controller must be able to demonstrate compliance with § 4, para. 1-7, including that personal data is processed in a manner that ensures sufficient security for the personal data in question, including protection against accidental loss, destruction or damage, using appropriate technical and organizational measures, cf. section 4, subsection. 7.

Thus, in addition to implementing appropriate technical and organizational security measures, the data controller must also be able to demonstrate compliance with these security measures.

The National Police has in its own statement acknowledged that during the investigation period no national guidelines have been prepared for how the police districts should handle and quality assure data received from the telecentre, which is why some police districts have prepared local guidelines for their processing of telecommunications information.

Furthermore, the National Police has acknowledged that there have been no system descriptions of the IT systems and databases used in the telecentre in connection with the handling of teledata.

In addition, the National Police has acknowledged that there has been no update of the organization's flow description since

2011, despite the solution has since been further developed, and that the National Police - in connection with the development of a new and more up-to-date system for converting and storing teledata - has not prepared project initiation document, business case, requirements specification or similar, which is otherwise the starting point in the National Police for the development or adaptation of already existing IT systems.

On the basis of the National Police's report, the Danish Data Protection Agency finds that the authority has not complied with the requirements of section 4 (1) of the Law Enforcement Act. 8, cf. § 4, para. 7, as the authority is not able to demonstrate written guidelines, guidelines or procedures for handling teledata, and thus can not demonstrate that the authority has ensured sufficient security for the personal data in question.

On that basis, the Danish Data Protection Agency finds that the National Police's processing of personal data has not taken place in accordance with the Law Enforcement Act, section 4, subsection. 8, cf. § 4, para. 7.

3.4. Summary

Overall, the Danish Data Protection Agency assesses that the National Police has had insufficient processes and workflows in connection with the processing of teledata. The Danish Data Protection Agency further finds that the National Police has not ensured the quality, accuracy and integrity of the delivered teledata, or has ensured the subsequent deletion of the information.

The Danish Data Protection Agency also assesses - on the basis of the National Police's statement - that the National Police has not taken appropriate technical and organizational security measures to ensure an appropriate level of security, including by ensuring that the authority does not process and pass on incorrect personal data. criminal cases.

In addition, the Danish Data Protection Agency assesses - on the basis of the National Police's statement - that there has been inadequate communication to the districts and further in the criminal case chain about known shortcomings in the content of data. This, together with the districts' unequal practice for quality control of data and a lack of managerial focus in the area, has led to in several cases incorrect personal information being provided, which is used as evidence in criminal cases.

On the basis of the above, the Danish Data Protection Agency finds grounds for expressing serious criticism that the National Police's processing of personal data has not taken place in accordance with section 27, section 4, subsection 1 of the Law Enforcement Act. 4 - 6 and § 4, para. 8, cf. 7.

The Danish Data Protection Agency also finds grounds for issuing an order to the National Police to delete the personal data that meet the requirements for deletion in accordance with the telecommunications centre's own guidelines, to the extent that

this has not already been deleted.

The order is issued pursuant to section 42 (1) of the Law Enforcement Act. 1.

The deadline for compliance with the order is 6 weeks from today's date. The Danish Data Protection Agency must request receipt of a confirmation that the National Police has sufficiently deleted the personal data in question.

The Danish Data Protection Agency draws attention to the fact that according to the Law Enforcement Act, section 50, subsection 2 shall be punished by a fine for failing to comply with an order issued in accordance with section 42.

In addition, the Danish Data Protection Agency must call on the National Police to draw up guidelines for deletions that are complied with, checked and sanctioned. This also applies to the data sets that have been passed on to requisitioners, and routines must be incorporated that ensure that all representations of data, at all stages of the organization, are deleted.

Concluding remarks

The Danish Data Protection Agency's decisions may not be appealed to another administrative authority, cf. section 42 (1) of the Law Enforcement Act. (2) The Authority's decisions may, however, be appealed to the courts, cf. section 63 of the Constitution.

The Danish Data Protection Agency will not take any further action in connection with this case.

However, the Danish Data Protection Agency must emphasize to the National Police that the Authority will monitor this processing area, and ensure that the National Police implements the necessary measures to ensure legal processing and satisfactory protection of the data subjects' rights.

The Danish Data Protection Agency must, for the sake of good order, note that the Authority expects to publish this statement on the Authority's website.

Appendix: Legal basis

Excerpt from Act no. 410 of 27 April 2017 on law enforcement authorities' processing of personal data with subsequent amendments (the Law Enforcement Act)

Chapter 1

Area of law

1. The Act applies to the processing of personal data by the police, the Public Prosecutor's Office, including the Military Public Prosecutor's Office, the Prison and Probation Service, the Independent Police Prosecuting Authority and the courts, wholly or

partly by automatic data processing, and other non-automatic processing of personal data contained or to be contained in a register when the processing is carried out for the purpose of preventing, investigating, revealing or prosecuting criminal offenses or enforcing criminal sanctions, including to protect against or prevent threats to public security.

PCS. 2. The Act does not apply to the processing of personal data carried out for or by the police and defense intelligence services.

PCS. 3. The Act does not apply to the processing of personal data pursuant to EU acts which entered into force on 6 May 2016 or before that date in the field of judicial cooperation in criminal matters and police cooperation, and which regulate the processing between the Member States and the designated authorities' access to EU information systems.

Rules on the processing of personal data in other legislation, which gives the data subject a better legal position, take precedence over the rules in this Act.

Chapter 3

Processing of information

4 pieces. The information processed shall be relevant and sufficient and shall not go beyond what is necessary to fulfill the purposes for which the information is collected and the purposes for which the information is subsequently processed.

PCS. The information processed must be accurate and, if necessary, up-to-date. Every reasonable step must be taken to ensure that personal data which are inaccurate in relation to the purposes for which they are processed are deleted or rectified immediately.

PCS. 5. The controller shall take all reasonable steps to ensure that personal data are not disclosed or made available if they are inaccurate, incomplete or out of date. To this end, the data controller verifies, as far as possible, the quality of the personal data before passing them on or making them available. In the context of the transfer of information, the necessary information shall be added as far as possible to enable the receiving competent authority to assess the extent to which the personal data are accurate, complete and reliable and the extent to which they are up to date. If it is found that incorrect personal data has been passed on or that personal data has been passed on illegally, this must be notified to the recipient immediately. The information must be corrected or deleted, or the processing must be restricted.

PCS. Collected information shall not be stored in a way that allows the data subject to be identified for a longer period of time than is necessary for the purposes for which the information is processed.

PCS. 7. Collected information shall be processed in a manner that ensures adequate security for the personal data in question, including protection against unauthorized or illegal processing and against accidental loss, accidental destruction or accidental damage, using appropriate technical or organizational measures, cf. 27.

PCS. The data controller is responsible for and must be able to demonstrate that para. 1-7 are observed.

Chapter 12

Treatment safety

27. The data controller and the processor shall, taking into account the current technical level, the implementation costs and the nature, scope, coherence and purpose of the processing and the varying probability and seriousness of the risks to the rights of natural persons, implement appropriate technical and organizational measures to ensure an appropriate level of security. these risks, in particular as regards the processing of the special categories of personal data covered by section 10.

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

[2] National Police Report, p. 62

[3] Statement, p. 62

[4] Statement, p. 62.

[5] Statement, p. 63.

[6] Statement, p. 63.

[7] Statement, p. 63.

[8] Statement, p. 64.

[9] Statement, p. 64.

[10] Statement, p. 64.

[11] Statement, p. 65.

[12] Statement, p. 65.

[13] Statement, p. 65.

[14] Statement, p. 66.

[15] Statement, p. 65.

[16] Statement, p. 67.

[17] Statement, p. 49.

[18] Statement, p. 67.

[19] Statement, p. 67.

[20] Statement, p. 67.

[21] Deloitte's study, p. 55.

[22] The Study, p. 33.

[23] Statement, p. 14.

[24] Statement, p. 15.

[25] The Study, p. 17.

[26] Statement, p. 81.

[27] Statement, p. 81.

[28] Statement, p. 85.

[29] The Study, p. 17.

[30] Statement, p. 86.

[31] The Study, p. 66.

[32] Statement, p. 87.

[33] The Study, p. 67.

[34] The Statement, p. 88.

[35] The Statement, p. 88.

[36] The Statement, p. 89.

[37] The statement, p. 89.

[38] The statement, p. 83.

[39] The Study, p. 30.

[40] The Study, p. 67.

[41] The Statement, p. 84.

[42] Statement, pp. 90-91.

[43] Statement, p. 91.

[44] Statement, p. 29.

[45] Statement, p. 52.

[46] The Study, p. 5.

[47] The Study, p. 55.

[48] The Study, p. 55

[49] The Statement, p. 23.

[50] Statement, p. 23.

[51] Statement, p. 24.

[52] Statement, p. 24.

[53] Statement, p. 71.

[54] Statement, p. 71.

[55] Statement, p. 72.

[56] Statement, p. 72.

[57] Statement, p. 72.

[58] Statement, p. 73.

[59] Statement, p. 73.

[60] Statement p. 24.

[61] The Danish Data Protection Agency's guide of July 2018 on data subjects' rights, p. 32.