Complaint about TDC's registration of traffic and location data

Date: 11-02-2019

Decision

Private companies

On the basis of a complaint about the registration of traffic and location data, the Danish Data Protection Agency expresses serious criticism that TDC's processing of personal data does not live up to the principle of data minimization.

J.nr. 2018-31-0070

The Danish Data Protection Agency hereby returns to the case where [complainant] on 22 August 2016 complained to the Danish Data Protection Agency about TDC A / S '(hereinafter TDC) processing of personal data about him in connection with TDC's registration of traffic and location data when the complainant's mobile phone the Internet.

Decision

After a review of the case, and after the case has been considered at a meeting of the Data Council, the Danish Data Protection Agency finds that there are grounds for expressing serious criticism that TDC's processing of personal data on complaints has not been in accordance with Article 5 of the Data Protection Regulation. PCS. 1, letter c.

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

2. Case presentation

It appears from the case that TDC has continuously registered information about complaints, including which mobile masts the complainant's mobile phone has connected to via internet communication. Complainants had become aware of these registrations based on a request for access to which TDC responded on 24 September 2015.

From the material received in connection with the insight, it appears that TDC over a period of 10 months performed 11,366 logging of location data by mobile data traffic. During the same period, 185 MMS CDR data were recorded.

On the basis of the above, the complainants on 9 and 11 February 2016 contacted the Danish Business Authority and complained about TDC's registration of traffic and location data for mobile data traffic.

In a reply to the Danish Business Authority on 1 April 2016, TDC has given a more detailed account of the registration of traffic and location data in question. The statement states, among other things. following:

“The basis for billing data for use in MMS (CDR) is formed in the part of the mobile network called MMSC (MMS center). This

data string contains i.a. a time stamp, but not registration of cell ID (mast locations).

In order to have a location (cell ID) linked to a specific MMS, TDC will have to collect location information from the traffic nodes in the so-called PS network. MMS is transported as data in the PS network, where it is not possible to distinguish between one and the other form of IP traffic. Therefore, the location of all mobile data traffic is collected.

Only by concatenating the time stamp of the MMS that is registered and stored in the settlement CDR with the corresponding [time stamp] in the collected data on mobile data from the traffic nodes can the location data for the MMS be separated.

TDC does not perform further data processing of location data and thus interconnection of MMS CDR and location information for mobile data until TDC receives a request from the police for disclosure of MMS location information, or when an end customer requests insight into the customer's own data under the Personal Data Act. Only with this merging of data is a match formed between the individual MMS and the collecting location.

It should be noted that TDC deletes location data when they are no longer relevant to store, cf. the Logging Order. In this way, TDC ensures that TDC can continue to store billing data for MMS in accordance with the [Accounting Act] (ie longer than one year), while location data is not stored longer than the logging executive order requires. If location was collected as part of the settlement CDR, TDC would not be able to delete location data from the settlement CDR until TDC can [delete] the settlement basis under the Accounting Act.

It should also be noted that TDC does not collect cell IDs for all the masts [that] a customer uses in connection with the use of mobile data (including MMS). TDC only collects registration of the cells used at the time when different state changes occur, eg if the customer has reached a specific volume limit, session start, end of session, when a data session has lasted one hour, or when changing radio technology (2G, 3G and 4G). This is the reason why [complainant] on his data extract can ascertain some periodic records. At the same time, this means that the registration of cell ID for an MMS does not necessarily correspond exactly to the cell to which the customer was associated when the MMS was sent, but the cell TDC last registered used in connection with the customer's use of mobile data communication. "

After initially - at the request of the Danish Data Protection Agency - having waited for the Danish Business Authority's processing of his complaint, on 5 April 2017, complainants again contacted the Danish Data Protection Agency, as the Danish Business Authority, among other things, had informed him that the board did not consider him to be a party to the board's case against TDC.

On 24 May 2017, the Danish Business Authority made a decision in the case before TDC and found in this connection that TDC's registration and storage of location data concerning mobile data traffic was not in breach of section 23, subsection. 1, in Executive Order no. 715 of 23 June 2011 on the provision of electronic communications networks and services (the tender notice).

The Danish Business Authority's decision states, among other things: that the Telecommunications Industry by letter of 12 November 2015 to the Danish Business Authority has stated that if the telecommunications providers are to separate location data for MMS communication from other mobile data, the sorting must take place before the collection of CDR files. The telecommunications industry has also stated that there are no equipment or techniques for this that the providers have at their disposal today, and that it will therefore require IT development to carry out such sorting. It is Teleindustriens loosely estimated estimate that such a change will in total cost a double-digit million amount for the industry, and that it will probably take approx. a year to implement such a solution.

Complainants have subsequently regained insight into their personal information at TDC.

From the material received, it appears that in the period 12 June 2017 - 11 June 2018, TDC performed 22,219 loggings of location data by mobile data traffic. During the same period, 20 MMS CDR data were recorded.

2.1. Complainant's remarks

Overall, the complainants have stated that TDC registers more information than is necessary to comply with TDC's obligation pursuant to section 4, no. 6 of the Executive Order on Logging.

Complainants have stated in this connection that only 1.6% of the registered information that TDC is obliged to register under section 4, no. 6 of the Logging Order. Complainants have further stated that in several cases his location was registered over a hundred times a day without him sending or receiving MMSs on those days.

Finally, complainants have referred to the fact that TDC can make an ongoing interconnection of MMS CDR information and the mobile data traffic, so that TDC only stores mobile data traffic that relates to MMS communication.

2.2. TDC's comments

TDC has stated that it appears from the guidance to section 1 of the Logging Order that telecommunications providers must only register and collect information on telecommunications traffic generated or processed in the provider's network, and that TDC is thus not required to develop special systems in order to provide relevant data that is not already processed in TDC's

mobile network.

TDC has further stated that the Minister of Justice, at the time of issuing the logging order, was aware that fulfillment of the requirement for logging of location data by MMS communication would result in a logging of location data for all mobile data traffic. In this connection, TDC has referred to the Telecommunications Industry's statement to the Ministry of Justice in connection with the creation of the Logging Order. The Ministry of Justice's consultation memorandum of 18 June 2004, pp. 34-35, states:

In many other cases, however, the requirements of the draft executive order create great doubt about the practical scope of the requirements for a specific service. For example, the guide gives the impression that location data (section 2, subsection 1, no. 6 of the Executive Order) must be registered in connection with communication via GPRS and in connection with the exchange of MMS. However, location data is not recorded in connection with said communications in most mobile networks. This is because the services in question are based on open logical channels that are physically activated as long as the terminal is switched on. The transport network is continuously updated in step with the customer's switch between cells, but this information is only used for a dynamic update of routing data. There is therefore no need or need for logging of location information for the individual communication. In cases where GPRS is used for, for example, messages at a higher level in relation to the mobile service - possibly. via an e-mail provider independent of the mobile service provider - there will be no registration of the communication in the mobile network apart from the [quantifications] of the volume consumption used for volume assessment. If location data is to be registered in connection with MMS and communication via GPRS in general, this can only be done by logging all cell information in connection with the logical channel used as a carrier and a subsequent temporal matching of these records with generated records for communication . This will be an extremely comprehensive task, and it will involve logging the customer's behavior independently of communications to and from the person in question. ”

In addition, TDC has stated that the company has investigated whether the technical development of the mobile networks since the issuance of the logging order has made it possible to register location data for MMS communication without registering location data for all mobile data traffic. However, this has not proved to be the case.

TDC further notes that an ongoing interconnection of location data for mobile data traffic and traffic data for MMS - in the company's view - will result in a compromise of the data basis that forms the basis for the location information provided to the police. Thus, in the event of a request for validation of data, TDC will not be able to review raw data in order to document that

the information is valid, as raw data no longer exists. Therefore, in TDC's opinion, it is necessary for TDC to store location data for all mobile data traffic in order to be able to provide valid location data for MMS communication after the logging order.

By letter dated 28 September 2018, TDC has stated that the MMS logging in question rests solely on TDC's flexibility and responsiveness to the Ministry of Justice's request to this effect, and that TDC does not have an independent interest in the logging in question.

Finally, TDC stated in a letter dated 7 November 2018 that TDC has stopped logging all location data for mobile data traffic and that all previously collected data has been deleted.

3. The competence of the Data Inspectorate

Pursuant to the Data Protection Act, section 27, subsection 1, the Danish Data Protection Agency supervises compliance with the general data protection rules contained in the Data Protection Regulation [1] and the Data Protection Act [2].

The supervision of rules on the processing of personal data that have not been replaced by special rules in e.g. telecommunications legislation, is thus with the Danish Data Protection Agency.

In a review of the tender notice, it is immediately only the provision in section 23, subsection Article 5 (5), which has content which gives rise to considerations regarding the relationship to the principle of data minimization in Article 5 (1) of the Data Protection Regulation. 1, letter c. The tender notice is as follows:

§ 23. Providers of public electronic communication networks or services must ensure that traffic data, cf. § 2, para. 1, no. 2, concerning subscribers or users is deleted or anonymised when they are no longer necessary for the transmission of the communication, cf. 2-5 and the Administration of Justice Act § 786, para. 4, or rules issued pursuant thereto.

PCS. 2. Notwithstanding subsection 1, a provider, as mentioned in para. 1, process and store traffic data for the purpose of charging subscribers and settling for interconnection. Such processing and storage of data is permitted until the expiry of the statutory limitation period for the debt obligations and settlements in question.

PCS. Notwithstanding subsection 1, a provider, as mentioned in para. 1, process traffic data, cf. section 2, subsection 1, no. 2, concerning subscribers or users with a view to marketing electronic communication services or the provision of additional services, cf. section 2, subsection 1, no. 4, provided that the subscriber or user has given his consent to this prior to the processing. Processing is only permitted to the extent and for the time required by the service or marketing. The subscriber or user must at any time have the opportunity to withdraw his consent.

PCS. Providers, as mentioned in para. (1) shall inform the subscriber or user of the types of traffic data that are processed for the purposes of the provisions of subsection (1). Purposes and the duration of the treatment referred to in paragraphs 2 and 3. In the case of processing for the purposes of the The purpose referred to in paragraph 3 must be notified before consent is obtained.

PCS. Providers, as mentioned in para. 1, shall ensure that the processing of traffic data as mentioned in para. 1-4 shall only be performed by persons who are employed by or act on the authorization of providers of public electronic communications networks or services, and who are engaged in billing or traffic management, processing complaints or other inquiries from subscribers, detecting fraud or marketing of the provider's own services or the provision of additional services. In connection with the processing of such specific cases, the processing of traffic data must be limited to only what is necessary for the processing of the case.

The provision thus contains in para. 5, last sentence, a principle of data minimization, which, however, only applies to situations where employees, etc. with telecommunications providers deals with specific cases, including complaints, fraud detection, etc., where the processing of traffic data in such specific cases must be limited to only what is necessary for the processing of the case.

Section 23 of the Executive Order on Public Procurement thus does not appear to contain a general principle of data minimization, which is why the provision does not - as a result of the principle of lex specialis - take precedence over Article 5 (1) of the Data Protection Regulation. 1, letter c.

Against this background, the Danish Data Protection Agency's assessment is that the Authority has the competence to address the question of whether TDC's processing of traffic and location data is in accordance with the basic principle of data minimization in Article 5 (1) of the Regulation. 1, letter c.

4. Registration of location data on complaints

4.1. Article 5 of the Data Protection Regulation

The processing of personal data must always be carried out in accordance with the basic principles set out in Article 5 of the Data Protection Regulation.

This means, among other things, that personal data must be sufficient, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimization"), cf. Article 5 (1) of the Regulation. 1, letter c.

4.2. The Logging Order

The Ministry of Justice's Executive Order no. 988 of 28 September 2006, as amended by Executive Order no. 660 of 19 June 2014 on providers of electronic communications networks and electronic communications services' registration and storage of information on telecommunications (the “Logging Order”) regulates the collection and storage of information on telecommunications with a view to the use of the information as part of the investigation and prosecution of criminal offenses. It follows from § 1 of the Logging Order that providers of electronic communications networks or services to end users must register and store information about telecommunications traffic generated or processed in the provider's network, so that this information can be used as part of the investigation and prosecution of criminal offenses. .

Section 4 of the Logging Order states the following:

“A provider of electronic communications networks or services to end users shall record the following information on landline and mobile telephony as well as SMS, EMS and MMS communications:

1) dialing number (A-number) and name and address of the subscriber or registered user,

2) dialed number (B-number) and name and address of the subscriber or registered user,

3) change of dialed number (C-number) and name and address of the subscriber or registered user,

4) receipt for receipt of messages,

5) the identity of the communication equipment used (IMSI and IMEI numbers),

6) the cell or cells to which a mobile telephone is connected at the start and end of the communication, as well as the exact geographical or physical location of the associated masters at the time of the communication,

The time of start and end of communication; and

8) the time of first activation of anonymous services (talk time card).

Of pkt. 6 of the general remarks to Act no. 378 of 6 June 2002, whereby the authorization provision in the Administration of Justice Act § 786, para. 4, was inserted, appears i.a. following:

“The proposed provision in the Administration of Justice Act § 786, para. 4, 1st sentence, cf. section 2, no. 3 of the Bill, and the administrative regulations laid down pursuant to the proposed provisions in section 786 (1) of the Administration of Justice Act. 4, 2nd sentence, and para. 5, could have certain negative economic and administrative consequences for the business community and the citizens. ”

Of the Minister of Justice's answer of 2 February 2012 to question no. 12 concerning the Bill amending the Penal Code, the Code of Judicial Procedure, the Competition and Consumer Affairs Act, the Arms Act, the Extradition Act and the Extradition Act to Finland, Iceland , Norway and Sweden. (Amendment of auditing provision) (L 53) from the Parliament's Legal Committee states the following about the financial consequences of the Logging Order:

“The Logging Order has been issued pursuant to section 786 (1) of the Administration of Justice Act. 4, according to which it is the responsibility of providers of telecommunications networks or telecommunications services to register and store for 1 year information on telecommunications traffic for the purpose of investigation and prosecution of criminal offenses.

The provision in the Administration of Justice Act § 786, para. 4, was inserted by Act no. 378 of 6 June 2002. It appears from the preparatory work for this (item 6 in the general remarks in Bill no. L 35) that it was known that the bill would entail certain additional costs for the business community. .

It follows from telecommunications legislation that providers of electronic communications networks or services to end-users free of charge to the state must ensure that the technical equipment and technical systems used by the provider are set up so that the police can access information on telecommunications traffic and to intervene in the secrecy of communications in the form of historical telecommunications information and extended telecommunications information in accordance with the rules in Chapters 71 and 74 of the Administration of Justice Act.

It is thus provided in the telecommunications legislation that the costs associated with arranging the systems in order to make interference with the secrecy of communications possible must be borne by the telecommunications providers.

With regard to the telecommunications companies' costs as a result of the logging order, the Ministry of Justice can state that the then Danish Commerce and Companies Agency in April 2011 - in connection with the reporting on the then government's objective of reducing administrative burdens - prepared an update of the AMVAB measurement (Activity-based Measurement of Corporate Administrative Burdens) in the area of the Ministry of Justice. With the update, an inventory was made of the development in the administrative burdens of the Ministry of Justice's business-oriented legislation for the period July 2005 to the end of 2010. The inventory is attached (available at www.amvab.dk).

Regarding the administrative burdens for the telecommunications companies in relation to the Logging Order, it appears from the statement (page 22) that the telecommunications companies have assessed that they have ongoing burdens for approx. 60 million It is stated that the burdens are distributed with approx. 50 mio. DKK regarding the operation of the current logging

systems and approx. 10 mio. DKK regarding depreciation of expenses for the development of new systems, which have been established to live up to the requirements of the Logging Order.

It may be added that the police reimburse the telecommunications providers for the actual expenses associated with the telecommunications providers' assistance in carrying out specific interventions in the secrecy of communications. ”

In a statement of 11 May 2017 to the Danish Business Authority, the Ministry of Justice has stated the following about the logging order:

“By letter dated 30 March 2017, the Danish Business Authority has requested an opinion from the Ministry of Justice on whether the Logging Order § 4, no. MMS, when it i.a. is assumed, 1) that the mobile operators must delete or anonymize location data traffic in accordance with section 23 (1) of the Executive Order on Public Procurement. 1, unless it follows from the logging order that the operators are obliged to register and store such data, and 2) that the technical design of the mobile operators' systems does not make it possible to separate location data for MMS from location data for certain other types of mobile data traffic.

Pursuant to the Administration of Justice Act, section 786, subsection 4, it is the responsibility of providers of telecommunications networks or telecommunications services to carry out registration and storage (logging) for 1 year of information on telecommunications traffic for use in the investigation and prosecution of criminal offenses. The Minister of Justice, after consultation with the Minister of Trade and Industry and the Minister of Energy, Climate and Supply, shall lay down detailed rules on this registration and storage.

Pursuant to the Administration of Justice Act, section 786, subsection 4, the logging order has been issued. The Executive Order lays down the detailed rules for the logging that the providers must carry out.

Section 1 of the Logging Order states that providers of electronic communications networks or services to end users must register and store information about telecommunications traffic generated or processed in the provider's network, so that this information can be used as part of the investigation and prosecution of criminals. relationship.

It is also stated in section 4, no. 6 of the Executive Order on Logging, that a provider of electronic communication networks or services to end users must register the following information on fixed and mobile telephony as well as SMS, EMS and MMS communication: “the cell or cells a mobile phone is connected to at the start and end of the communication, as well as the corresponding geographical or physical location of the associated masters at the time of the communication. ”

In this connection, the Ministry of Justice must state that it is explicitly stated in section 4, no. 6 of the Logging Executive Order that providers must log location information by MMS traffic, and that the executive order does not make assumptions about the design of providers' technical systems. The provision in § 4, no. 6 of the Logging Order, on logging location information by MMS traffic, thus applies regardless of the design of the providers' technical systems and thus also if the specific systems used by the providers are arranged so that in connection with logging of MMS traffic also logs certain additional location data during mobile data traffic.

In this connection, the Ministry of Justice must note that since the tender notice falls under the Ministry of Business Affairs and the Ministry of Energy, Climate and Supply, the Ministry of Justice has no basis for deciding whether section 23 of the tender order on deletion or anonymisation of traffic data provides grounds for requiring that in the light of the logging rules, the mobile operators' systems must be technically designed in a way that makes it possible to separate location data for MMS traffic from location data for certain other types of mobile data traffic.

The Ministry of Justice can finally state that the ministry is currently working on a bill to revise the logging rules. In this connection, it is expected that the requirements for the telecommunications providers' logging of location information for data traffic other than MMS traffic will be explicitly addressed. It is expected that the bill on the revision of the logging rules will be presented in the parliamentary year 2017-18. ”

By letter dated 28 November 2018, the Danish Data Protection Agency requested a supplementary opinion for the understanding of the above-mentioned opinion of 11 May 2017. In this connection, the Danish Data Protection Agency stated, among other things:

”[The Danish Data Protection Agency immediately understands] The Ministry of Justice's statement of 11 May 2017 so that telecommunications providers are required by section 4, no. 6 of the Logging Order, to register location data for MMS communication, regardless of the design of telecommunications providers' IT systems legislation other than the Logging Order, which sets (other) requirements for the construction of telecommunications providers' IT systems, including the processing of information in this connection. "

In response to the Danish Data Protection Agency's request, the Ministry of Justice stated in a letter dated 10 December 2018:

“On this occasion, the Ministry of Justice must announce that the Ministry has no comments on the Danish Data Protection Agency's understanding of the Ministry's statement of 11 May 2017 to the Danish Business Authority. The Ministry can thus

refer to the fact that the Ministry, as stated in the opinion, did not find a basis for deciding whether section 23 of the Executive Order on the deletion or anonymisation of traffic data provides a basis for requiring telecommunications providers' systems to be technically arranged in the light of logging rules. in a way that makes it possible to separate MMS traffic location data from location data for certain other types of mobile data traffic. ”

4.3. Justification for the Danish Data Protection Agency's decision

Overall, TDC has stated that it has been necessary to register location data for all mobile data traffic in order to comply with the Logging Order's requirement for registration of location data for MMS communication, as the technical structure of TDC's mobile network does not allow registration data for MMS alone. communication without simultaneously registering location data for all mobile data traffic.

Following a review of the case, the Danish Data Protection Agency's assessment is that the construction of TDC's IT system cannot justify non-compliance with the data protection rules, just as any costs associated with establishing new systems that make it possible to register the necessary information alone cannot justify non-compliance with data protection rules.

It is thus the Data Inspectorate's assessment that TDC's processing of personal data, which TDC has not been obliged to register in accordance with the Logging Order, has been in breach of Article 5 (1) of the Data Protection Regulation. 1, letter c, on data minimization.

In this connection, the Danish Data Protection Agency has placed special emphasis on the fact that the vast majority of the information that TDC has registered about complaints has not been necessary to comply with TDC's obligations under the Logging Order, as only 1.6% and 0.09% of the registered information, respectively, TDC has registered complaints The two times complainants have exercised their right to request access to their personal information with TDC, related to MMS communication.

The Danish Data Protection Agency has also emphasized that the information was registered solely due to the structure of TDC's mobile network, and that TDC itself has stated that TDC has no purpose in registering the excess information in question.

Furthermore, the Danish Data Protection Agency has emphasized that it was already argued by Teleindustrien in connection with the issuance of the Logging Order that it would be costly for telecom providers to develop systems that only register the necessary information, but that the Logging Order was nevertheless issued in its current form.

Furthermore, the Danish Data Protection Agency's assessment is that an ongoing interconnection of location data for mobile data traffic and traffic data for MMS will not be a sufficient measure in order to comply with the basic principle of data minimization in Article 5 (1). 1, letter c.

The Danish Data Protection Agency has hereby emphasized that, until the time of the merger, TDC will continue to have collected a large amount of excess information, for which TDC has no purpose.

The Danish Data Protection Agency has also noted that TDC has stated that the company no longer registers the information in question.

5. Concluding remarks

The Danish Data Protection Agency hereby considers the case closed and does not take any further action in the case.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (General data protection regulation).

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