Completion of planned inspection at Viborg Municipality

Date: 05-08-2019

Decision

Public authorities

The Danish Data Protection Agency has expressed serious criticism that Viborg Municipality has not complied with the requirements of the Data Protection Ordinance in connection with the use of data processors.

Journal number: 2018-423-0022

Summary

Viborg Municipality was among the authorities that the Danish Data Protection Agency had selected for inspection in 2018. The inspections focused in particular on the municipalities' compliance with the requirements associated with the use of data processors.

In connection with the audit, the Danish Data Protection Agency has expressed serious criticism that Viborg Municipality has not complied with the requirements of the Data Protection Ordinance in connection with the use of data processors, cf. Article 28 (1) of the Data Protection Ordinance. 3, and Article 5, para. Article 5 (2) The Danish Data Protection Agency has also issued an injunction to Viborg Municipality to enter into data processor agreements that meet the requirements of Article 28 (1) of the Regulation. 3, with regard to five of the municipality's data processors.

The Danish Data Protection Agency's final statement states, among other things, that Viborg Municipality had not entered into data processor agreements with five of the municipality's data processors, where the agreement - as a minimum - contained a description of the obligations mentioned in Article 28 (1). 3.

In addition, it appears from the statement that the municipality had not continuously supervised the processing of personal data at - at least - three of the municipality's data processors, just as the municipality had not continuously supervised the processing of personal data at the municipality's sub-processors.

You can read the Danish Data Protection Agency's guide on data controllers and data processors here.

You can read the Danish Data Protection Agency's guiding text on supervision of data processors and sub-data processors here.

You can find the Danish Data Protection Agency's standard data processor agreement here.

Decision

Viborg Municipality was among the public authorities selected by the Danish Data Protection Agency in the autumn of 2018 for supervision in accordance with the Data Protection Act [1] and the Data Protection Ordinance [2].

The Data Inspectorate's planned inspection of Viborg Municipality focused in particular on the municipality's compliance with the requirements associated with the use of data processors.

At the request of the Danish Data Protection Agency, Viborg Municipality had sent a list of which data processors the municipality uses before the inspection visit. Viborg Municipality had - at the request of the Authority - also sent a copy of all of the municipality's data processor agreements.

The inspection visit took place on 8 November 2018.

On the basis of what the Danish Data Protection Agency has established in connection with the inspection visit, the Danish Data Protection Agency finds grounds for concluding in summary:

That Viborg Municipality in several cases has not complied with the requirements of Article 28 (1) of the Data Protection Regulation. 3, including by

that the municipality in respect of 5 of the municipality's data processors has not entered into data processor agreements which - as a minimum - contain a description of the obligations mentioned in Article 28, para. 3,

that the municipality in several cases has not sufficiently related to how the obligations in Article 28, para. 3 must be fulfilled by the parties in practice,

that the municipality has not instructed all data processors in a sufficiently clear manner in which processing of personal data is to be carried out on behalf of the municipality.

That Viborg Municipality has not continuously supervised the processing of personal data by - at least - 3 of the municipality's data processors.

That Viborg Municipality has not continuously supervised the processing of personal data by the municipality's sub-data processors.

Following a review of the case, the Danish Data Protection Agency finds grounds to express serious criticism that Viborg Municipality has not complied with the requirements of the Data Protection Ordinance in connection with the use of data processors, cf. Article 28 (1) of the Data Protection Ordinance. 3, and Article 5, para. Article 5 (2)

The Danish Data Protection Agency also finds grounds for issuing an injunction to Viborg Municipality to enter into data processor agreements that meet the requirements of Article 28 (1) of the Regulation. 3, with the following data processors:

[Data Processor]

[Data Processor]

[Data Processor]

[Data Processor]

[Data Processor]

The order is issued pursuant to Article 58 (1) of the Data Protection Regulation. 2, letter d.

The deadline for compliance with the order is 30 September 2019. The Danish Data Protection Agency must request no later than the same date to receive a confirmation that the order has been complied with.

According to the Data Protection Act, section 41, subsection 2, no. 5, is punishable by a fine or imprisonment for up to 6 months for anyone who fails to comply with an order issued by the Danish Data Protection Agency pursuant to Article 58 (1) of the Data Protection Regulation. 2.

In addition, the Danish Data Protection Agency must request Viborg Municipality for an account of the data protection law considerations that the municipality has made on the basis of the inspection visit. The statement must be received by the Danish Data Protection Agency no later than 30 September 2019.

The Danish Data Protection Agency must finally request Viborg Municipality to send a concrete and detailed plan for how the municipality will in future carry out the necessary supervision of the municipality's data processors and sub-data processors. The plan is to be received by the Danish Data Protection Agency no later than 15 October 2019.

In choosing the sanction, the Danish Data Protection Agency has found it mitigating that the five data processor agreements that Viborg Municipality - at the time of the inspection visit - had not managed to enter into / update, only make up a small part of the municipality's total number of around 130 data processor agreements. The Danish Data Protection Agency has thus taken into account that the municipality should have entered into / updated a large number of data processor agreements before 25 May 2018, where the data protection regulation applied, and that entering into and negotiating data processor agreements can generally be a comprehensive and time-consuming process. .

In relation to Viborg Municipality's supervision of data processors, the Danish Data Protection Agency has emphasized the

information that the municipality generally carries out a risk-based supervision of the treatments carried out by the municipality's data processors, even though the samples showed that the municipality's supervision was deficient.

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

1. Conclusion of data processor agreements, the principle of accountability and the general principles for the processing of personal data

1.1. Relevant rules

Article 28 (1) of the Data Protection Regulation 3, it follows that the processing of a data processor must be governed by a contract or other legal document in accordance with EU law or the national law of the Member States, which is binding on the data processor with respect to the data controller and which determines the subject and duration of the processing, the nature and purpose of the processing, the type of personal data and the categories of data subjects and the obligations and rights of the data controller. This contract or other legal document shall in particular cover the requirements for the data processor set out in Article 28 (2) of the Regulation. 3, letter a-g.

Pursuant to Article 28 (1) of the Data Protection Regulation, 3, litra a, b.a. a data processor agreement states that the data processor may only process personal data in accordance with documented instructions from the data controller, including in relation to the transfer of personal data to a third country or an international organization, unless required by EU or national law by the data processor; is subject to; in that case, the data controller shall inform the data controller of this legal claim before processing, unless the court in question prohibits such notification for reasons of important societal interests.

It follows from Article 29 of the Data Protection Regulation that the data controller and anyone performing work for the data controller or processor and who has access to personal data may only process this data on the instructions of the data controller, unless required by EU law or the national law of the Member States. right.

Pursuant to Article 28 (1) of the Data Protection Regulation, Article 28 (3) (d) further states in a data processor agreement that the data processor must meet the conditions referred to in Article 28 (2). 2 and 4, to make use of another data processor (sub-data processor).

Article 28 (1) of the Data Protection Regulation 2, it follows that the data processor may not make use of another data processor (sub-data processor) without prior specific or general written approval from the data controller. In the case of general written approval, the data controller shall notify the data controller of any planned changes regarding the addition or

replacement of other data processors and thereby give the data controller the opportunity to object to such changes.

Of Article 28, para. 4, it follows that if a data processor uses another data processor (sub-data processor) in connection with the performance of specific processing activities on behalf of the data controller, this other data processor is imposed the same data protection obligations as those stipulated in the contract or another legal document between the controller and the processor as referred to in paragraph Through a contract or other legal document under EU law or the national law of the Member States, in particular providing the necessary guarantees that they will implement the appropriate technical and organizational measures in such a way that the processing meets the requirements of this Regulation. If this other data processor does not fulfill its data protection obligations, the original data processor remains fully responsible to the data controller for the fulfillment of this other data processor's obligations.

It also follows from Article 5 (1) of the Data Protection Regulation 1, letters a and f, that personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject, and that the data must be processed in a way that ensures adequate security of the personal data in question, including protection against unauthorized or illegal processing and against accidental loss, destruction or damage, using appropriate technical and organizational measures.

In addition, it follows from Article 5 (1) of the Data Protection Regulation That the data controller is responsible for and must be able to demonstrate that Article 5, para. 1 is complied with.

Article 5 (1) of the Data Protection Regulation 2, thus contains a responsibility principle, which means that the data controller i.a. must ensure and be able to demonstrate that personal data is processed for lawful and reasonable purposes and that the data is processed in a way that ensures adequate security for the personal data in question - even when the data controller asks another party (a data processor) to process the data on his behalf.

The data controller must then - in order to live up to his obligations in connection with the use of data processors - draw up a data processor agreement which regulates the areas mentioned in Article 28 (1). 3, and relate to how these obligations are to be fulfilled in practice.

The data controller must also - in a sufficiently clear manner - instruct the data processor in what processing of personal data is to be carried out on behalf of the data controller. In practice, this will mean that the data controller must have an overview of the processing and be able to document which processing activities the data processor is instructed to carry out, including which activities the data controller has approved in relation to any transfers to third countries or international organizations. use

of sub-processors, etc.

The existence of a sufficiently clear instruction is - in the opinion of the Danish Data Protection Agency - a prerequisite for the data controller to have an overview and control of the processing when this is left to a data processor, and to be able to determine when a data processor may acts outside the scope of the agreed instruction.

It is also important that the data controller is aware of whether it appears from the agreement that the data processor also uses the information for its own purposes. If the data controller approves a data processor agreement, which states - either in the data processor agreement, in the main agreement or other terms of the agreement - that the data processor uses the information for its own purposes, in the Authority's view it will be a transfer of personal data. Chapter 2.

If personal data is passed on to the data processor, this can advantageously be regulated in a separate supplement to the agreement, so that the data processor's processing for its own purposes is not mixed with the processing carried out on behalf of the data controller. Thus, it should be clear when the data processor is subject to instructions from the data controller and when the data processor is independently responsible for the processing of personal data.

1.2. Compliance with the rules at Viborg Municipality

1.2.1. Data processor agreements in process or during update

During the inspection visit, the Danish Data Protection Agency asked whether Viborg Municipality has entered into valid data processor agreements with all its data processors, or whether there are agreements that have not yet been entered into or updated so that they meet the minimum requirements in the Data Protection Ordinance.

In this connection, the Danish Data Protection Agency referred to the fact that it appears from the submitted list of data processors that there are 19 data processor agreements which are in process or which are being updated.

Viborg Municipality noted that in the specific cases, data processor agreements exist, but that these have not yet been updated in relation to the new requirements. The municipality also stated that it must be assessed whether some of these data processor agreements should simply terminate, for example in cases where there is no data processor construction or where the processing has ceased.

Following the inspection visit, Viborg Municipality has sent an updated list of the municipality's data processor agreements by e-mail dated 11 December 2018. It appears from this that the municipality lacks to enter into valid data processor agreements with five of the municipality's data processors.

During the review of the specific data processor agreements, the Danish Data Protection Agency also asked about the following points.

1.2.2. The type of personal data processed on behalf of the municipality

During the review of the specific data processor agreements, the Danish Data Protection Agency found examples that the agreement did not state which specific types of personal data are processed on behalf of the municipality. Some agreements thus contained a more general indication that the processing of personal data is in accordance with the Data Protection Regulation or similar.

The Danish Data Protection Agency noted that in general it should be clearer which types of personal data are left to the data processor.

In this connection, however, the Danish Data Protection Agency agreed that in certain special situations it may be difficult to determine in advance which specific types of personal data are covered by the agreement. This may, for example, be the case when processing personal data in relation to an e-mail server or a cloud service, where many different types of information will be processed, e.g. because a municipality must use the service to store cases from several different disciplines.

In such a situation, one must - in the opinion of the Danish Data Protection Agency - try to specify as specifically as possible the types of personal data that are the subject of processing. However, it will of course depend on a specific assessment of how specifically it is possible in the data processor agreement to specify the type of personal data.

During the inspection visit, the Danish Data Protection Agency noted that it should in any case be clear whether information of a sensitive or confidential nature is being processed, as this will have an impact on, for example, the establishment of security measures and the data controller's ongoing supervision of the data processor.

1.2.3. The procedure for the municipality's approval or objection to the use of new sub-data processors

During the inspection visit, the Danish Data Protection Agency asked more about the procedure for the municipality's approval of sub-data processors.

During the review of the specific agreements, the Danish Data Protection Agency thus asked whether it has been agreed in detail how and when the municipality should be notified of planned changes - when the municipality has given a general approval for the use of sub-processors - including whether the municipality has the opportunity to object to any changes.

Based on the municipality's responses, the Danish Data Protection Agency was able to establish that in several cases no

decision had been made on how and when the data processor should notify the municipality of such changes.

In one of the cases where the parties to the data processor agreement had taken a position on the practical implementation of the notification, it could also be stated that the time period between the notification and the planned use of the data processor was agreed to such a short period that the municipality would not be able to manage to object to the use.

The Danish Data Protection Agency noted in this connection that - in the Authority's view - it would not be in accordance with the requirements of Article 28 (1) of the Data Protection Regulation. 2, that a data processor transfers the processing or parts of the processing to a sub-data processor before the data controller has actually had the opportunity to object to this. The Danish Data Protection Agency also stated that it is the Authority's immediate perception that the data controller must be actively notified of changes regarding the addition or replacement of sub-data processors.

1.2.4. Documented instructions and the data processor's processing of personal data for own purposes

During the inspection visit, the Danish Data Protection Agency generally asked how the municipality assesses whether a documented instruction is sufficiently clear.

The municipality stated that the data processor typically describes the processing that is performed, as the data processor is an expert in the service provided, but that the municipality actively relates to the description of the processing that the data processor has prepared.

The Danish Data Protection Agency then asked what considerations the municipality has made in relation to the cases where it appears from a data processor agreement that the data processor will also use information for its own purposes, including whether the municipality is aware of this situation.

In this connection, the Danish Data Protection Agency stated that the Authority has previously experienced / seen examples of data processor agreements, from which it is more or less clear that the data processor also uses the information for its own purposes.

The municipality stated that they had not experienced such situations and that the municipality would otherwise have reacted to this.

After the general questions, the Danish Data Protection Agency asked about the municipality's considerations in relation to the instructions in some of the selected data processor agreements.

Data Processor 1

The Danish Data Protection Agency asked whether the municipality had made any considerations in relation to the data processor using personal data for its own purposes. In this connection, the Danish Data Protection Agency referred to Annex 3 of the agreement (instructions), which states that:

“The municipality and the municipality's teachers must be aware that [data processor] uses selected information for their own purposes. [Data Processor] uses e.g. information on user behavior to be able to target the user-oriented dialogue as well as to optimize our products and services. [Data Processor] will therefore process selected information in connection with newsletters, market and product surveys as well as service and product orientations ”.

The municipality stated that the municipality was not aware of this when entering into the agreement, and therefore did not take an active part in the data processor's use of the personal data for its own purposes.

When asked, the municipality stated that they have thus not investigated which specific personal information the data processor uses for their own purposes, just as the municipality has not commented on whether there is a transfer authority.

The municipality then confirmed that it is not clear to the municipality when the data processor acts on behalf of the municipality and when they act on their own behalf. The municipality stated that they would follow up on this after the inspection visit.

Data Processor 2

During the inspection visit, the Danish Data Protection Agency asked in more detail up to point 2 in the service description (an appendix to the data processor agreement), which states that the data processor is entitled to change the service description on an ongoing basis, which i.a. contains points concerning the description of the subject of the agreement, the type of personal data, the purpose of the processing, security measures, the use of sub-processors and transfers to third countries.

It also appears from the service description that the data processor must notify changes in this in "such time" that the municipality can object to the changes. The municipality then has 30 days to object. If the municipality does not object within 30 days, the data processor will consider the changes to be accepted by the municipality.

In this connection, the Danish Data Protection Agency questioned whether a lack of objection from the municipality could constitute a documented instruction in relation to the processing by the data processor.

Data Processor 3

In relation to the data processor agreement with data processor 3, the Danish Data Protection Agency noted that - in the

Authority's view - it is unclear what processing the data processor carries out on behalf of the municipality and what the data processor may do as an independent data controller.

The municipality noted that the data processor stores the personal information on behalf of the municipality, and that the data processor is a so-called data warehouse.

The Danish Data Protection Agency noted that, based on the content of the terms - and the many associated documents - it is immediately unclear whether the data processor is anything other than a data warehouse, and that - in the Authority's view - it is difficult to discern the processing that takes place.

The municipality stated during the inspection visit that the municipality agreed that it is a "maze" to find your way around the many documents to which the terms refer, and confirmed that the municipality has not read all the documents.

After the inspection visit, Viborg Municipality referred to the following sections in relation to clarification of the instructions.

“Processing of customer data, ownership

Customer data is used or otherwise processed only to provide Online Services to the Customer, including purposes in connection with the provision of such services. [Data Processor] does not use or otherwise process Customer Data or derive information therefrom for advertising or similar commercial purposes. As between the parties, the Customer retains all rights, ownership and interest in and to Customer Data. [Data Processor] does not acquire any rights in Customer Data, except for the rights that the Customer grants to [Data Processor] for the purpose of providing Online Services to the Customer. This section does not affect [data processor]'s rights to software or services for which [data processor] licenses the Customer. ”

and

”Roles and responsibilities for therapist and data controller

Customers and [data processor] accept that the Customer is responsible for the registration of Personal Data, and [data processor] is the processor of such data, except when (a) the Customer acts as a processor of Personal Data, in which case [data processor] is a sub-processor, or (b) otherwise stated in the terms and conditions specific to the Online Services. [Data Processor] only processes Personal Data according to documented instructions from the Customer. Customer agrees that its volume license agreement (including Terms of Online Services) together with Customer's use and configuration of functions in the Online Services is Customer's complete and final documented instructions to [Data Processor] regarding the processing of Personal Data. All additional or amended instructions must be agreed in accordance with the change process for the

Customer's volume license agreement. In the event that the Personal Data Ordinance applies and the Customer is a processor, the Customer guarantees to [data processor] that the Customer's instructions, including the appointment of [data processor] as a processor or sub-processor, have been approved by the relevant data controller. ”

and

“Preservation and deletion of data

Throughout the period in which the Customer's subscription is active, the Customer has the opportunity to access and extract and delete Customer Data stored on each Online Service.

[Data Processor] retains Customer Data, which remains stored on the Online Services (excluding free trial and LinkedIn services), in an account with limited functionality for 90 days after the Customer's subscription expires or expires, so that the Customer can extract the data. When the 90-day retention period ends, [Data Processor] will deactivate Customer's account and delete Customer Data and Personal Data within a further 90 days, unless [Data Processor] has permission or is required by applicable law to retain such data or has been authorized to do so. in this Agreement.

The online service may not support the storage or extraction of software provided by the Customer. [Data Processor] has no liability in connection with the deletion of Customer Data or Personal Data as described in this section. "

After reading the above section, it is still not clear to the Danish Data Protection Agency what processing of personal data the data processor carries out on behalf of Viborg Municipality.

1.2.5. The municipality's overview of the use of sub-data processors and the transfer of personal data to third countries

During the inspection visit, the Danish Data Protection Agency repeatedly asked the municipality's overview in relation to specific data processors' use of sub-data processors whether the municipality had accepted the transfer of personal data to third countries in the specific cases and whether the municipality had ensured that a valid transfer basis existed.

In several cases, Viborg Municipality could not answer the above questions, and it was clear to the Danish Data Protection Agency that the municipality lacks an overview.

1.3. Summary

In relation to point 1, the Data Inspectorate's summary is that Viborg Municipality has not complied with Article 28 (1) of the Data Protection Ordinance. 3.

The Danish Data Protection Agency has hereby emphasized that, with regard to 5 of the municipality's data processors, Viborg

Municipality has not entered into data processor agreements which - as a minimum - contain a description of the obligations mentioned in Article 28 (1). And in several cases has also not sufficiently related to how the obligations in Article 28, para. 3 must be fulfilled by the parties in practice.

In addition, the Danish Data Protection Agency has emphasized that Viborg Municipality - in relation to all of the data processor agreements reviewed - has not instructed the data processors in a sufficiently clear manner in which processing of personal data is to be carried out on behalf of the municipality. This is made particularly clear by the municipality's lack of overview of what they have accepted in relation to the use of sub-data processors and the transfer of personal data to third countries. With regard to one of the data processor agreements reviewed, it was also the Data Inspectorate's opinion that the municipality was not aware that they had accepted the data processor's use of personal data for its own purposes, and that the municipality had not assessed whether there was the necessary transfer authority for a such acceptance.

2. Supervision of the processing of personal data by the municipality's data processors

2.1. Relevant rules

Article 5 (1) of the Data Protection Regulation 1, it follows, among other things, that personal data must be processed legally, fairly and in a transparent manner in relation to the data subject, and that the data must be processed in a way that ensures adequate security for the personal data in question, including protection against unauthorized or illegal treatment and against accidental loss, destruction or damage, using appropriate technical and organizational measures.

In addition, it follows from Article 5 (1) of the Data Protection Regulation That the data controller is responsible for and must be able to demonstrate that Article 5, para. 1, is complied with.

Article 5, para. 2, contains a principle of accountability, which - in the opinion of the Danish Data Protection Agency - means that the data controller must ensure and be able to demonstrate that personal data is processed for lawful and reasonable purposes, and that the data is processed in a way that ensures adequate security of the personal data - also when the data controller asks another party (a data processor or sub-data processor) to process the information on his behalf.

Failure to follow up on the processing of personal data that takes place at data processors and sub-processors will - in the opinion of the Data Inspectorate - basically mean that the data controller can not ensure or demonstrate the processing's compliance with the general principles for processing personal data, including that the data is processed on a lawful, fair and transparent in relation to the data subject ('legality, fairness and transparency') and that the data is processed in a way that

ensures adequate security of the personal data in question, including protection against unauthorized or illegal processing and against accidental loss; destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality').

The data controller must thus carry out (greater or lesser) supervision of compliance with the data processor agreements entered into, including e.g. that the data processor has implemented the agreed technical and organizational security measures. [3]

2.2. Compliance with the rules at Viborg Municipality

During the inspection visit, the Data Inspectorate asked whether the municipality generally supervises the data processors' compliance with the requirements in the data processor agreement, including how often and how supervision is carried out.

Viborg Municipality stated that the municipality has a risk-based approach to data protection, and that the municipality generally requires an audit statement from the data processor. Some of the declarations must be actively accessed by the municipality itself and downloaded from the supplier's website, others will be sent to the municipality by the data processor.

The Danish Data Protection Agency asked whether inspections are carried out in other ways than by obtaining / receiving audit statements.

In addition, the municipality stated that in cases where it is not possible to obtain / receive an audit statement, the municipality instead collects information by telephone discussion with the specific data processor, which is based on the topics from ISAE 3000.

When asked about this, Viborg Municipality stated that the municipality has not documented the inspections where the municipality has collected information by telephone discussion with the data processors, for example by journaling a telephone note.

When asked, Viborg Municipality further stated that the municipality generally uses the audit statements ISAE 3402 and ISAE 3000 when they supervise the handling of personal data by the data processor. The municipality confirmed that these statements primarily concern the processing security of the data processor.

2.2.1. Random check

During the inspection visit, the Danish Data Protection Agency also carried out a random check of whether Viborg Municipality had obtained audit statements in relation to the processing of personal data by three specific data processors.

On the basis of the random checks, the Danish Data Protection Agency was able to establish that Viborg Municipality could not present any of the selected samples in documentation for obtaining audit statements, or exercising other forms of ongoing supervision of the processing at the data processor.

The Danish Data Protection Agency has noted that after the inspection visit, Viborg Municipality has submitted audit statements obtained from the three data processors in question and documentation that the municipality has related to the content of these.

2.3. Summary

In relation to point 2, the Data Inspectorate's summary is that Viborg Municipality has not sufficiently complied with Article 5 (1) of the Data Protection Ordinance. 2, cf. 1.

The Danish Data Protection Agency has emphasized that Viborg Municipality has continuously supervised the processing of personal data at - at least - the 3 of the municipality's data processors, which the Data Inspectorate had selected for random checks, and that the municipality has thus not ensured or been able to demonstrate compliance with the processing. of the general principles set out in Article 5 (1) of the Regulation. 1.

Supervision of the processing of personal data by the municipality's sub-data processors

3.1. Relevant rules

See point 2.1 of this opinion.

3.2. Compliance with the rules at Viborg Municipality

During the inspection visit, the Data Inspectorate asked until whether the municipality generally follows up on whether the processing of any sub-data processors takes place in accordance with the terms that follow from the municipality's agreement with the data processor.

Viborg Municipality stated in this connection that the municipality must approve the use of sub-data processors either by a general or specific approval

The Danish Data Protection Agency stated that the approval of any sub-data processors does not in itself constitute a (ongoing) supervision of the processing of personal data by the sub-data processor. On that basis, the Danish Data Protection Agency asked in more detail how the municipality ensures that the processing by the sub-data processor is in accordance with the data processor agreement and the regulation.

The municipality referred to the chain responsibility, where the data processor is liable for the sub-processor's violations of the data processor agreement.

Viborg Municipality then stated that the municipality on that basis does not supervise the processing of the sub-data processors.

The Danish Data Protection Agency agreed that the supervision of the processing of personal data by the sub-processor will often take place through the data processor, but that this in itself does not exempt the data controller from - to a greater or lesser extent - finding out whether the processing as a whole lives up to the rules of the Regulation.

The Danish Data Protection Agency then asked whether the municipality ensures - for example by inserting a requirement to this effect in the data processor agreement - that the data processor carries out the relevant supervision of the sub-data processor.

Viborg Municipality stated that the municipality uses audit statements, which to a certain extent affect the data processor's supervision of the sub-processor. The municipality confirmed, however, that it is not generally a requirement in the municipality's data processor agreements that the data processor must carry out the necessary supervision of any sub-data processors.

The Danish Data Protection Agency noted that the processing of the sub-processors' processing can take place, for example, by inserting the requirement for the data processor's supervision of the sub-processors in the data processor agreement, and that the data processor then sends documentation of the performed inspection to the data controller or makes it easy for the data controller to obtain information. .

When asked, the municipality confirmed that they can not be sure whether the data processor supervises the sub-data processor, as this is not agreed in the data processor agreement, and as the municipality has not followed up on whether this actually happens.

The municipality noted, however, that they generally trust that their suppliers are in control of the processing of any sub-data processors.

3.3. Summary

In relation to point 3, the Data Inspectorate's summary is that Viborg Municipality has not complied with Article 5 (1) of the Data Protection Ordinance. 2, cf. 1, by not having sufficiently followed up on the processing of personal data that takes place at the

municipality's sub-data processors.

The Danish Data Protection Agency has emphasized that Viborg Municipality has not ensured that the processing of personal data by the sub-processors is carried out on an ongoing basis, for example by inserting this as a requirement in the data processor agreement and then actively following up on whether there is in fact supervision and what these inspections show about the treatment. Viborg Municipality has thus not ensured or been able to demonstrate the treatments' compliance with the general principles in Article 5 (1) of the Regulation. 1.

4. Conclusion

On the basis of what the Danish Data Protection Agency has established in connection with the inspection visit, the Danish Data Protection Agency finds grounds for concluding in summary:

That Viborg Municipality in several cases has not complied with Article 28 (1) of the Data Protection Ordinance. 3, including by that the municipality in respect of 5 of the municipality's data processors has not entered into data processor agreements which - as a minimum - contain a description of the obligations mentioned in Article 28, para. 3,

that the municipality in several cases has not sufficiently related to how the obligations in Article 28, para. 3 must be fulfilled by the parties in practice,

that the municipality has not instructed all data processors in a sufficiently clear manner in which processing of personal data is to be carried out on behalf of the municipality.

That Viborg Municipality has not continuously supervised the processing of personal data by - at least - 3 of the municipality's data processors.

That Viborg Municipality has not continuously supervised the processing of personal data by the municipality's sub-data processors.

Following a review of the case, the Danish Data Protection Agency finds grounds to express serious criticism that Viborg Municipality has not complied with the requirements of the Data Protection Ordinance in connection with the use of data processors, cf. Article 28 (1) of the Data Protection Ordinance. 3, and Article 5, para. Article 5 (2)

The Danish Data Protection Agency also finds grounds for issuing an injunction to Viborg Municipality to enter into data processor agreements that meet the requirements of Article 28 (1) of the Regulation. 3, with the following data processors:

[Data Processor]

[Data Processor]

[Data Processor]

[Data Processor]

[Data Processor]

The order is issued pursuant to Article 58 (1) of the Data Protection Regulation. 2, letter d.

The deadline for compliance with the order is 30 September 2019. The Danish Data Protection Agency must request no later than the same date to receive a confirmation that the order has been complied with.

According to the Data Protection Act, section 41, subsection 2, no. 5, is punishable by a fine or imprisonment for up to 6 months for anyone who fails to comply with an order issued by the Danish Data Protection Agency pursuant to Article 58 (1) of the Data Protection Regulation. 2.

In addition, the Danish Data Protection Agency must request Viborg Municipality for an account of the data protection law considerations that the municipality has made on the basis of the inspection visit. The statement must be received by the Danish Data Protection Agency no later than 30 September 2019.

The Danish Data Protection Agency must finally request Viborg Municipality to send a concrete and detailed plan for how the municipality will in future carry out the necessary supervision of the municipality's data processors and sub-data processors. The plan is to be received by the Danish Data Protection Agency no later than 15 October 2019.

In choosing the sanction, the Danish Data Protection Agency has found it mitigating that the five data processor agreements that Viborg Municipality - at the time of the inspection visit - had not managed to enter into / update, only make up a small part of the municipality's total number of around 130 data processor agreements. The Danish Data Protection Agency has thus taken into account that the municipality should have entered into / updated a large number of data processor agreements before 25 May 2018, where the data protection regulation applied, and that entering into and negotiating data processor agreements can generally be a comprehensive and time-consuming process. .

In relation to Viborg Municipality's supervision of data processors, the Danish Data Protection Agency has emphasized the information that the municipality generally carries out a risk-based supervision of the treatments carried out by the municipality's data processors, even though the samples showed that the municipality's supervision was deficient.

[1] 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).

[2] 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).

[3] Read more about this in the Danish Data Protection Agency's guiding text on supervision of data processors and sub-data processors, which can be found on the Authority's website.