

Supervision of the Danish Immigration Service's supervision of a data processor

Date: 15-12-2022

Decision

Public authorities

No criticism

Supervision / self-management case

Data processor

Basic principles

The Home Travel Agency's supervision of a data processor did not give rise to criticism.

Journal number: 2021-421-0101

Summary

The Danish Data Protection Authority has carried out a written inspection of the Home Travel Agency's supervision of one of the agency's data processors.

The Danish Data Protection Authority found no reason to override the Danish Immigration Service's assessment that the agency's supervision of UIM Koncern IT in the form of insight into UIM Koncern IT's security and data protection through ongoing dialogue, and a starting point in annual reports from the Ministry of Immigration and Integration's data protection adviser and from UIM Koncern IT itself, and any reactions to the extent that the supervision of UIM Koncern IT gives rise to this, constitutes an appropriate supervision of the data processor.

Decision

1. Written supervision of the Home Travel Agency's supervision of data processors

The Returning Agency was among the authorities that the Danish Data Protection Authority had selected in autumn 2021 to supervise according to the data protection regulation[1] and the data protection act[2].

The Danish Data Protection Authority's inspection was a written inspection which focused on the Danish Immigration Service's inspection of data processors.

By letter of 8 November 2021, the Danish Data Protection Authority notified the Danish Agency for Home Travel. In this connection, the Danish Data Protection Authority requested to be sent a list of data processors to whom the Migration Agency

entrusts sensitive and/or confidential personal data.

On 29 November 2021, the Home Travel Agency appeared with a list of the agency's data processors.

On the basis of the list, the Danish Data Protection Authority chose to carry out an inspection of the Danish Migration Agency's supervision of the agency's data processor UIM Koncern It (hereafter KIT).

On 8 December 2021, the Danish Data Protection Authority requested the Norwegian Travel Agency to provide information on: the agency's plan for its supervision of KIT, including considerations about frequency and what is being supervised whether the agency has supervised KIT how the agency has followed up on any completed inspections of KIT.

Against this background, the Returning Agency sent a statement on the matter on 19 January 2022.

On 12 July 2022, the Danish Data Protection Authority requested a supplementary statement in the case, which the Danish Travel Agency issued on 9 August 2022.

2. Decision

After a review of the case, the Danish Data Protection Authority finds no basis for overriding the Home Travel Agency's assessment that the agency's supervision of the data processor KIT has been carried out in accordance with the rules in Article 5, paragraph 1 of the Data Protection Regulation. 2, cf. subsection 1.

Below follows a closer review of the case and a rationale for the Data Protection Authority's decision.

3. Case presentation

At the outset, the Home Travel Agency has stated that the agency was established on 1 August 2020 and in that connection has taken over a number of tasks from authorities in both the Ministry of Immigration and Integration's group (hereafter UIM) and the Ministry of Justice's group. The Immigration Agency's primary IT supplier is KIT, located in UIM's department, and Statens It. As a starting point, the Travel Agency does not use other IT suppliers or data processors.

The National Board of Repatriation has stated that KIT, as a data processor for the agency, manages the agency's IT, including the agency's central record and case processing systems, databases and communication solutions. KIT has access to personal data in connection with e.g. maintenance, operation of the middleware and the application layer as well as support. KIT, on behalf of the Home Travel Agency, processes information about identity, portrait photos, marital status, citizenship and nationality, travel route, employment, information about family, union membership, information about asylum law matters,

e-mail address, telephone number, address, case numbers, personal ID, information about social relations , salary information, information about religious or philosophical beliefs, health information, biometric data for the purpose of identification, sexual relations, social security numbers and information about criminal convictions and offences.

3.1. Background and plan for supervision of UIM Group It

The Norwegian Migration Agency has informed the case that KIT is a joint IT function in UIM that manages central IT systems on behalf of all authorities in UIM's group.

The individual authorities in UIM's group are independent data controllers, and KIT is organizationally placed in UIM's department. The authorities in UIM's group have therefore assessed that the relationship between KIT and the individual agencies, including the Home Travel Agency, are data processing relationships. The framework for the Home Travel Agency's supervision of KIT is therefore laid down in a data processing agreement between the Home Travel Agency and KIT.

The chosen supervision model reflects the fact that the National Travel Agency and KIT are group-related, and that there is therefore significantly closer cooperation between the data controller and the data processor than in a typical supplier relationship. The National Board of Repatriation thus has ongoing dialogue with KIT in connection with a large number of committee meetings, cooperation meetings, participation in IT projects, etc. The Home Travel Agency thereby gains an insight into KIT's handling of security incidents, supplier relationships and other topics related to security and data protection, which in a typical supplier relationship would require very frequent supervision.

The supervision model is also inspired by the supervision that the Danish Financial Supervisory Authority's Office for Audit and Supervision conducts with Statens IT on behalf of the customers. Supervision is thus based on annual reports from the department's data protection advisor and from KIT itself.

The Danish Travel Agency has stated that the department's data protection advisor annually prepares a report on data protection in the department, including in KIT. In addition, KIT annually prepares a status report for the information security work. Both reports are submitted to UIM's IT committee, where the Danish Travel Agency is represented at executive level.

The Danish Immigration Service's information security team, which also includes the Danish Agency's data protection advisor, reviews the reports with a particular focus on subjects of importance for information security and data protection in the Danish Immigration Service. Reviewing the reports is included as a regular task in the information security team's annual cycle.

The reports are typically drawn up during the first quarter, and the Home Travel Agency's supervision is carried out thereafter.

The Danish Migration Agency has stated that the status of information security is a fixed point at the meetings of UIM's IT committee. IT committee meetings are held at regular intervals, typically six times a year. Here, KIT typically informs about major security incidents, results of external inspections, cooperation with subcontractors, awareness efforts and the like. Material for the IT committee meetings is reviewed by the Home Travel Agency's information security team before the meetings, with a particular focus on topics of importance for information security and data protection in the Home Travel Agency.

In addition, the Home Travel Agency has stated that if the agency - in connection with the review of the annual reports, meetings in the IT committee or cooperation with KIT in general - becomes aware of conditions that the Home Travel Agency wishes to be further elucidated or documented, the Home Travel Agency will make proposals to the IT committee. The IT committee then makes a decision on the inspection. Concrete or themed supervision can be carried out both on the basis of material submitted to UIM's IT committee, security incidents identified or other risks identified by the Immigration Agency. It is the opinion of the Danish Travel Agency that the above-mentioned form of supervision provides adequate control of the data processing at KIT, including with a view to ensuring that the data processing agreement and the data protection legal requirements are complied with.

3.2. Carried out inspections

The Home Travel Agency has informed the case that since its establishment in August 2020, the agency has participated in UIM's IT committee. Furthermore, since the establishment of the team in October 2020, the agency's information security team has provided comments on topics of importance for information security and data protection in the Migration Agency before all meetings of the IT committee. The ongoing supervision of information security in connection with these meetings has thus been carried out since the end of 2020.

In its opinion of 19 January 2022, the National Board of Repatriation stated that the board had just reviewed the report from the department's data protection advisor for 2021. KIT's report on information security for 2021 had not yet been completed. The Home Travel Agency would carry out a review of KIT's annual report in accordance with the information security team's supervision plan when it was available, expected during the first quarter of 2022.

In its statement of 9 August 2022, the Immigration Agency has stated that on 4 and 5 August 2022 the agency reviewed the annual report from KIT and compared it with the annual report from the Ministry of Immigration and Integration's DPO for 2021.

At the end of the inspection, the agency subsequently prepared a report with conclusions.

In this connection, the Norwegian Migration Agency has stated that the agency expected the annual report from KIT during the first quarter of 2022, and the agency therefore notified this to the Danish Data Protection Authority on 19 January 2022. The annual report was delayed, which is why the Norwegian Migration Agency was in dialogue with KIT about this, i.a. for the purposes of the Agency's supervision. On 16 June 2022, KIT sent the annual report to the National Travel Agency, but due to a regrettable processing error, the agency only reviewed the annual report on 4 and 5 August 2022.

3.3. Follow-up after supervision

In its statement of 19 January 2022, the Danish Home Repatriation Agency has informed the case that the agency continuously follows up on security issues of relevance to the agency and is in close dialogue with KIT and UIM's department on this matter. Among other things, the National Travel Agency has been in dialogue with KIT about the handling of security incidents on the systems managed by KIT on behalf of the agency.

Follow-up on inspections is a fixed part of the Norwegian Home Travel Agency's procedure for supplier management. To the extent that inspections of KIT give rise to reactions on the part of the Home Travel Agency, follow-up will take place in accordance with these procedures.

4. Reason for the Data Protection Authority's decision

It follows from the data protection regulation article 28, subsection 1, that a data controller may only use data processors who can provide the necessary guarantees that they will implement the appropriate technical and organizational measures in such a way that the processing meets the requirements of the data protection regulation and ensures protection of the data subject's rights.

Of the data protection regulation, article 24, subsection 1, it appears that the data controller must implement appropriate technical and organizational measures to ensure and to be able to demonstrate that the processing is in accordance with the regulation.

The data controller must thus be able to demonstrate that the data processor provides sufficient guarantees for the implementation of technical and organizational measures that meet the requirements of the data protection regulation and ensure protection of the data subject's rights. This detection must be possible throughout the treatment process over time, which i.a. can be done by controls.

This appears from the data protection regulation's article 5, subsection 1, letter a, that personal data must be processed legally, fairly and in a transparent manner in relation to the data subject ("legality, fairness and transparency").

Furthermore, it follows from the regulation's article 5, subsection 1, letter f, that personal data must be processed in a way that ensures sufficient security for 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 ("integrity and confidentiality").

In addition, it follows from the data protection regulation article 5, subsection 2, that the data controller is responsible for and must be able to demonstrate that Article 5, subsection 1, is observed.

Article 5, subsection 2, contains an accountability principle which – in the Danish Data Protection Authority's view – 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 sufficient security for the personal data in question – also when the data controller asks another party (a data processor or sub-processor) to process the information on its behalf.

Lack of follow-up on the processing of personal data by data processors and sub-processors will – in the opinion of the Danish Data Protection Authority – basically mean that the data controller cannot ensure or demonstrate that the processing complies with the general principles for the processing of personal data, including that the data is processed on a legal, fair and transparent manner in relation to the data subject ("lawfulness, fairness and transparency"), and that the information is processed in a way that ensures sufficient security for 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").

In October 2021, the Danish Data Protection Authority published new, practically applicable guidance on how data controllers can carry out such inspections^[3]. It appears from the guidance that the greater the risks there are for the data subjects in the processing by the data processor, the greater the demands placed on the data controller's supervision of the data processor.

This applies both in relation to how the data controller must carry out supervision and how often this must take place.

After a review of the case, the Danish Data Protection Authority finds no basis for overriding the Home Travel Agency's assessment that the agency's supervision of the data processor KIT has been carried out in accordance with the rules in

Article 5, paragraph 1 of the Data Protection Regulation. 2, cf. subsection 1.

The Danish Data Protection Authority has hereby placed emphasis on the fact that the Swedish Travel Agency – since the Swedish Travel Agency and KIT are group-affiliated – has an ongoing dialogue with KIT in connection with IT committee meetings, collaboration meetings, participation in IT projects, etc., and that, based on the information provided in this connection, the Swedish Travel Agency receives a insight into KIT's handling of security incidents, supplier relationships and other topics related to security and data protection, which in a typical supplier relationship would require very frequent supervision.

The Danish Data Protection Authority has also emphasized that the Swedish Migration Agency has reviewed the UIM's data protection advisor's report for 2021 on data protection in the department, including in KIT, that the Swedish Migration Agency has reviewed KIT's annual status report for the information security work for 2021, that the Swedish Migration Agency's information security team, according to the information, reviews the reports with a special focus on topics of importance for information security and data protection in the Swedish Travel Agency, and that follow-up on inspections is a fixed part of the Swedish Travel Agency's procedure for supplier management.

The Danish Data Protection Authority thus finds no reason to override the Danish Home Travel Agency's assessment that the agency's supervision of KIT in the form of insight into KIT's security and data protection through ongoing dialogue, and a starting point in annual reports from UIM's data protection advisor and from KIT itself, and any reactions to that extent the supervision of KIT gives rise to this, constitutes an appropriate supervision of the data processor.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons in connection with the processing of personal data and on the free exchange of such data and on the repeal of Directive 95/46/EC (general regulation on data protection).

[2] Act No. 502 of 23 May 2018 on supplementary provisions to the Regulation on the protection of natural persons in connection with the processing of personal data and on the free exchange of such information (the Data Protection Act).

[3]

https://www.datatilsynet.dk/Media/637710957381234368/Datatilsynet_Vejledning%20om%20tilsyn%20med%20databehandlere_oktober-2021.pdf