Supervision of the Board of International Recruitment supervision of two data processors

Date: 16-12-2022

Decision

Public authorities

Criticism

Data processor

Basic principles

The Board for International Recruitment's supervision of two data processors gave rise to criticism.

Journal number: 2021-421-0102

Summary

The Danish Data Protection Authority found that there was a basis for criticizing the fact that the Agency for International Recruitment (hereafter SIRI) supervised two data processors, Keesing Reference Systems and Thales Danmark A/S, not in accordance with the data protection rules. The Danish Data Protection Authority has emphasized that SIRI did not supervise the data processor Keesing Reference Systems in 2021, and that the agency in relation to the data processor Thales A/S had not taken measures to ensure that the Danish Immigration Service's supervision of the data processor also covered SIRI's interests.

After a review of the specific circumstances in the case, the Norwegian Data Protection Authority assessed that Thales A/S' processing of personal data on behalf of SIRI has been regulated by a contract in accordance with the Data Protection Regulation, Article 28, subsection 3.

Decision

1. Written supervision of SIRI's supervision of data processors

The Agency for International Recruitment and Integration (hereafter SIRI) 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 supervision was a written supervision which focused on SIRI's supervision of data processors.

By letter of 8 November 2021, the Norwegian Data Protection Authority notified the supervisory authority of SIRI. In this connection, the Danish Data Protection Authority requested to be sent a list of data processors to whom SIRI entrusts sensitive and/or confidential personal data.

SIRI appeared on 29 November 2021 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 SIRI's supervision of the agency's data processors Keesing Reference Systems and Thales Denmark A/S (hereafter Thales).

On 8 December 2021, the Danish Data Protection Authority requested SIRI to provide information on:

the agency's plan for its supervision of Keesing Reference Systems and Thales, including considerations about frequency and what is being supervised

whether the agency has supervised the selected data processors

how the agency has followed up on any completed inspections of the data processors.

Against this background, SIRI sent a statement on the matter on 24 January 2022. The statement gave rise to the Danish Data Protection Authority to ask a number of questions about SIRI's supervision of the two data processors by letter of 17 February 2022. SIRI replied to the letter on 8 March 2022.

By e-mail of 21 April 2022, the Danish Data Protection Authority asked SIRI to disclose the agency's plan for supervision of Thales. Against this background, SIRI issued a supplementary opinion on the matter on 10 May 2022.

2. Decision

After a review of the case, the Danish Data Protection Authority finds that there is a basis for expressing criticism that SIRI's processing of personal data has not taken place in accordance with the rules in the data protection regulation, article 5, subsection 2, cf. subsection 1.

It is the Danish Data Protection Authority's assessment that Thales' processing of personal data on behalf of SIRI has been regulated by a contract in accordance with the data protection regulation's article 28, subsection 3.

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

3. Case presentation

3.1. Keesing Reference Systems

It appears from the case that Keesing Reference Systems is a supplier of Keesing scanners, which are part of SIRI's ID control

in the EU and international recruitment area. The Keesing scanner is used as a supplement to assess the authenticity of ID documents, including passports, ID cards, etc. that belong to citizens who are either applicants or references in a residence case. In connection with the use of the Keesing scanner, Keesing Reference Systems processes the data that is loaded into the scanners for the purpose of assessing authenticity. In this connection, Keesing Reference Systems processes information about name, nationality, address, date of birth, place of birth, gender, height, date of issue, date of expiry, biometric data in the form of portrait photo from ID card, passport or similar and possibly national identification number.

SIRI has provided the following information about the background and plan for supervision of Keesing Reference Systems:

"SIRI has drawn up a supervision plan for the agency's supervision of the data processor Keesing Reference Systems. The supervision plan stipulates, as a starting point, that SIRI supervises the data processor by asking the data processor for an annual declaration/report carried out by an independent third party. SIRI orients itself in the statement/report, and assesses on that basis whether SIRI should initiate further supervisory steps, as SIRI has reserved the possibility of other forms of supervision (ad hoc supervision and physical supervision).

The supervision plan has been created on the basis of the supplier's documented level of information security management, the criticality of the asset and the other risks associated with the processing. Furthermore, the conclusions from carried out risk assessments are included in the deliberations on which form of supervision is best suited to the relationship between SIRI and the data processor.

In connection with entering into the data processing agreement, an ISO baseline risk assessment and a Privacy Impact Assessment (PIA) were made. The PIA assessment has shown that the processing generally involves a medium to high risk for the registered, as the system is used for processing e.g. passport information that can be used for e.g. identity theft. Considering that the supplier is ISO-certified, which expires on 12 August 2022, it is SIRI's assessment at the present time that the form of supervision with obtaining an annual audit carried out by an independent third party provides an adequate control of the data processing at the data processor.

SIRI has stated that they have carried out inspections of Keesing Reference Systems in the summer of 2020. During the inspection, an audit report was obtained, which SIRI reviewed, and then SIRI assessed that the data processor's processing of personal data on SIRI's behalf was satisfactory.

SIRI has also carried out an ad-hoc inspection of Keesing Reference Systems in January 2022 in relation to the data

processor's compliance with the instructions given in the data processor agreement regarding the deletion of personal data. The background for the ad-hoc inspection was that SIRI became aware of Keesing Reference Systems' non-compliance with the data processing agreement's instructions on deleting personal data after 30 days. This was because the data processor believed that a formal annex outside the data processing agreement needed to be signed. SIRI signed the declaration in January, although the agency was of the opinion that the instructions in the data processing agreement were clear and distinct. Keesing Reference Systems now deletes data in accordance with the deletion instructions in the data processing agreement. SIRI has stated that the agency has not carried out the planned annual inspection of Keesing Reference Systems in 2021 due to a major organizational change in SIRI and Citizen Service, which is the responsible professional office for the data processing agreement with Keesing Reference Systems. The organizational change meant a merger of several offices, restructuring in SIRI and in the individual offices, including Citizen Service in particular. Borgerservice is now in the process of carrying out the annual inspection of Keesing Reference Systems in 2022 and will soon obtain an audit report from an independent third party.

3.2. Thales Denmark A/S

It appears from the case that Thales processes data on behalf of SIRI in connection with the production and delivery of residence cards to foreigners. In this connection, Thales processes information about name, date of birth, address, type of permit, personal ID, nationality, place of birth, place of issue, date of issue, expiration date, gender, biometric data for the purpose of unique identification in the form of a portrait photo, signature and fingerprint for storage in a biometric chip on the residence card, social security numbers and information about the application at the Ministry of Immigration and Integration. SIRI has stated that the agency has been in dialogue with Thales about entering into a data processing agreement since autumn 2020, when the agency became aware that no data processing agreement had been concluded between SIRI and Thales. The work has dragged on as the data processor has not wanted to enter into a data processing agreement with SIRI, as SIRI is not to be considered a party to the main contract. Until 2021, SIRI has used the main contract concluded between the Swedish Immigration Service and Thales, since SIRI was part of the Swedish Immigration Service in 2011, when the contract was concluded.

SIRI is per 21 January 2022 formally joined as a party to the main contract of 2 November 2011 between the Danish Immigration Service and Thales. SIRI also has per 18 January 2022 entered into a data processing agreement with Thales.

Prior to the formalization of the agreement between Thales, the Danish Immigration Service and SIRI, it was SIRI's view that the agency was covered by the main contract of 2 November 2011 between Thales and the Danish Immigration Service as part of the joint group cooperation.

In addition, SIRI has stated that the agency's responsibilities were separated from the Danish Immigration Service (then the Immigration Service) in 2012, after which they were transferred to the newly created Agency for Detention and Recruitment (SFR). In 2014, SFR was combined with the Labor Market Agency in the newly created Agency for Labor Market and Recruitment (STAR). In 2015, the departmental duties were separated from STAR into an independent agency, the Agency for International Recruitment and Integration, which has since taken its current form under the Ministry of Immigration and Integration, where the Immigration Service is also located.

Until autumn 2020, it has thus been SIRI's opinion, on the basis of group-wide cooperation and a certain shared IT infrastructure, that the supply agreement between the Danish Immigration Service and Thales - including the associated data processing agreement - was sufficiently comprehensive with regard to the production of residence cards on SIRI's territory.

In this connection, SIRI has stated that since autumn 2020, when the above was deemed inappropriate, it has tried several times to enter into a separate data processing agreement with Thales, which succeeded on 18 January 2022 as part of SIRI entering into the main contract with Thales on 21 January 2022.

SIRI has stated that until 2020 the Agency considered the Danish Immigration Service as a supervisor with Thales, which is why SIRI assessed that the Agency did not have its own responsibility as a supervisor. SIRI has therefore not entered into agreements with the Danish Immigration Service regarding supervision of the data processor, and SIRI has not taken measures to ensure that the Danish Immigration Service's supervision covered SIRI's interests. SIRI has familiarized itself with the Danish Immigration Service's written inspection and gap analysis with the data processor in 2020, in which questions were asked regarding the data processing agreement, technical and organizational measures, including whether personal data is deleted in accordance with the data processing agreement.

In this connection, SIRI has also stated that the agency has prepared a vulnerability assessment in early 2021 as part of the identification of potential vulnerabilities in connection with SIRI's business of issuing residence cards. Part of the vulnerability assessment showed that Thales' checks and handling of errors in the production of residence cards appear to be fully adequate at first glance. The assessment here was that data security was generally acceptable. SIRI had therefore not

planned any further supervision following the vulnerability assessment.

In addition, SIRI has stated that the agency has also not supervised Thales independently of the Danish Immigration Service. This must be seen in the light of the fact that SIRI has recently entered into a party to the main contract and that in January 2022 SIRI has entered into a data processing agreement with Thales.

It appears from the data processor agreement that SIRI can annually carry out a written inspection of the data processor and/or a physical inspection of the data processor's premises. In continuation of the entered into data processing agreement, SIRI has worked on developing a plan for SIRI's supervision of Thales in the 1st quarter of 2022.

SIRI has subsequently stated that the agency has drawn up a plan for supervision of Thales based on the criticality of the system and the other risks associated with the treatment.

SIRI has stated that the supervision plan is based on the fact that SIRI has entered into the main agreement between the Danish Immigration Service and Thales, that the Danish Immigration Service and SIRI have roughly the same deliveries, that the Danish Immigration Service and SIRI use the same systems to process and transfer information to Thales for use for the production of residence cards, and that the data processing agreement between SIRI and Thales is almost identical to the Danish Immigration Service's data processing agreement with Thales.

Against this background, SIRI has assessed that a large part of the supervision need with Thales can be covered by SIRI reviewing the Danish Immigration Service's supervision of the supplier's compliance with the agencies' data processing agreements. The inspection is carried out based on the Danish Immigration Service's inspection concept, in which a plan for inspection of the supplier is determined on the basis of annual gap analyses.

In connection with the above form of supervision, SIRI prepares independent supplementary questions for Thales based on annual assessments of risks on a number of characteristics including, among other things, security incidents in connection with the supplier's data processing for SIRI. SIRI considers that it is necessary for the agency to ask follow-up supervisory questions to Thales, as it is conceivable that in the relationship with the supplier, e.g. may be security incidents that do not concern the Danish Immigration Service. SIRI expects to carry out inspections in the 3rd quarter of 2022.

In addition, SIRI will carry out ad-hoc supervision according to the circumstances, including e.g. in the event of significant technical and/or organizational changes at the supplier or in the event of major security incidents, etc.

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.

It is further stated in the guidance that a supervision based on a documented supervision of the data processor carried out by an independent third party is a way for the data controller to carry out appropriate supervision when the data processor processes sensitive or confidential information about many data subjects on behalf of the data controller. This can either be done by a statement prepared by an independent third party, such as an auditor's statement, or by using another party's supervision, e.g. an authority that supervises on behalf of several authorities.

It also appears from the guidance that the data controller in that connection, i.a. must ensure that the supervision covers the processing activities of the data controller at the data processor.

4.1.

After a review of the case, the Danish Data Protection Authority finds that there are grounds for expressing criticism that SIRI's supervision of the data processors Keesing Reference Systems and Thales has not taken place in accordance with the rules in the data protection regulation, article 5, subsection 2, cf. subsection 1.

The Danish Data Protection Authority has thereby emphasized that SIRI did not supervise Keesing Reference Systems in 2021.

The Danish Data Protection Authority has also emphasized the fact that SIRI has for a period used Thales as a data processor, without SIRI having taken measures to ensure that the Danish Immigration Service's supervision covered SIRI's interests.

The Danish Data Protection Authority also finds no basis for overriding SIRI's assessment that the agency's supervision of the data processor Keesing Reference Systems constitutes an appropriate supervision of the data processor.

The Danish Data Protection Authority has hereby emphasized that SIRI has drawn up the supervision plan based on a risk assessment of the processing carried out by Keesing Reference System on behalf of SIRI, and that the supervision is carried out by SIRI obtaining an annual statement/report prepared by an independent third party, and that SIRI orients itself in the statement/report and, on that basis, assesses whether further supervisory steps should be initiated.

Furthermore, the Danish Data Protection Authority finds no basis for overriding SIRI's assessment that a large part of the supervisory need with Thales can be covered by SIRI reviewing the Danish Immigration Service's supervision of Thales' compliance with the agencies' data processing agreements.

The Danish Data Protection Authority has thereby emphasized the information that SIRI has included in the assessment of the supervision plan, that the Danish Immigration Service and SIRI have roughly the same deliveries, that the agencies use the same systems to process and transfer information to Thales for use in the production of residence cards, and that the data processing agreement between SIRI and Thales is almost identical to the Danish Immigration Service's data processing agreement with Thales.

Furthermore, the Danish Data Protection Authority has emphasized that SIRI, in the form of supervision, also prepares independent supplementary questions for Thales based on annual assessments of risks, including e.g. security incidents in connection with Thales' data processing on behalf of SIRI.

4.2.

This appears from the data protection regulation's article 28, subsection 3, that a data processor's processing must be regulated 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 regard to the data controller, and which determines the object and duration of the processing, the processing nature and purpose, the type of personal data and the categories of data subjects, as well as the data controller's obligations and rights.

It is the Danish Data Protection Authority's assessment that Thales' processing of personal data on behalf of SIRI has been regulated by a contract in accordance with Article 28, subsection 3.

The Danish Data Protection Authority has emphasized the specific circumstances of the case, including that since 2011 there has been a main contract with an associated data processing agreement between the Danish Immigration Service and Thales, which regulated Thales' processing of personal data, that SIRI was part of the Danish Immigration Service at the time the main

contract was entered into, that Thales' processing of personal data on behalf of SIRI – in the opinion of the Danish Data Protection Authority – appears to be a continuation of the same processing activity that was originally carried out on behalf of the Danish Immigration Service (production and delivery of residence cards), and that the processing activity has been transferred from the Danish Immigration Service to SIRI as part of ministerial reshuffles.[4]

The Danish Data Protection Authority has noted that SIRI has since assessed that it is most appropriate for there to be an independent data processing agreement between SIRI and Thales, and that SIRI entered into an independent data processing agreement with Thales in January 2022.

[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

[4] The assessment is, among other things, based on an analogy of the Danish Data Protection Authority's statement with j.nr. 2013-212-0137, which can be found on the authority's website: https://www.datatilsynet.dk/afgoerelser/historiske-afgoerelser/2013/dec/vedroerende-behandling-af-personspresningen-i-verbindelse-med-grenspaltning