Serious criticism of PrivatBo in case of lack of processing security

Date: 25-04-2022

Decision

Private companies

Serious criticism

Reported breach of personal data security

Treatment safety

Sensitive information

Unintentional disclosure

Social Security number

The Danish Data Protection Authority expresses serious criticism of PrivatBo for having passed on tenants' confidential information. The Danish Data Protection Authority has previously proposed a fine in the case, which was closed by the police due to a mistake.

Journal number: 2019-441-1480

Summary

The Danish Data Protection Authority has made a decision in a case where the Danish Data Protection Authority has assessed that the management company PrivatBo A.M.B.A. of 1993, has not met the data protection regulation's requirement to implement an appropriate level of security.

In 2018, PrivatBo – as a management company – assisted a housing fund with a planned sale of three properties. In this connection, PrivatBo provided material for the residents of the properties in question, a total of 424 USB keys. However, PrivatBo was not aware that documents containing personal data of a confidential nature and which should not have been disclosed were attached to part of the material provided.

The Danish Data Protection Authority reported PrivatBo to the police on 4 August 2020 and proposed a fine of DKK 150,000 based on the breach. On 14 December 2020, however, the investigation was mistakenly discontinued and the criminal case closed by the police on the basis of a mix-up of several circumstances. The police have stated that the case cannot be reopened.

Therefore, the Danish Data Protection Authority now expresses serious criticism that PrivatBo did not meet the requirements of the data protection regulation to implement appropriate technical and organizational security measures to ensure that the information was not passed on.

Decision

The Danish Data Protection Authority hereby returns to the case where PrivatBo A.m.b.A. of 1993 (hereinafter PrivatBo) on 23 December 2018 and by follow-up on 8 January 2019 reported a breach of personal data security to the Danish Data Protection Authority.

1. Decision

After a review of the case, the Danish Data Protection Authority finds grounds for expressing serious criticism that PrivatBo's processing of personal data has not taken place in accordance with the rules in the data protection regulation[1] article 32, subsection 1.

Below follows a review of the circumstances of the case and a detailed justification for the Data Protection Authority's decision.

2. Case presentation

2.1. Proceedings of the case

PrivatBo is a property and administration company that manages housing funds and leases in the capital for, among others, Frederiksberg Boligfond.

In 2018, PrivatBo assisted Frederiksberg Boligfond in connection with a planned sale of the properties Peter Bangs Hus, Svalegården and Den Sønderjyske By.

This follows from Section 100, subsection of the Tenancy Act. 1, that the lessor, in connection with the sale of properties that are wholly or partly used for living, must offer the tenants the property for takeover on a cooperative basis before handing it over to another party (obligation to offer). In continuation of this duty to offer, it follows from Section 103, subsection of the Tenancy Act. 4, that the owner, at the latest at the same time as the offer, must provide usual information about the property, including, among other things, information about the property's tenancy.

PrivatBo assisted Frederiksberg Boligfond with the preparation of material in connection with due-diligence, partly in relation to an impartial buyer, partly in connection with the obligation to offer, including gathering the information about the properties' rental conditions so that these could be handed over.

In this connection, PrivatBo has stated that when preparing the material for use for due diligence and fulfilling the obligation to offer, a virtual data room was created with material relating to the three properties, including lease contracts for all leases. The purpose of the data room was to exchange documents and data. PrivatBo has stated that 54 people have had access to the data room, including the buyer of the properties as well as legal advisers, financial advisers, insurance advisers, economic advisers and architects.

A total of 424 USB keys were then prepared with the relevant material for the specific property, including tenancies linked to the property. 39 social security numbers appeared on the USB keys, just as there was sensitive personal data in the form of health information on the USB keys handed out to the tenants in the property "Peter Bangs Hus".

PrivatBo has stated that the mentioned USB keys with material were distributed to the tenants in the three properties on 21 December 2018 in the period between 10.00 and at 12.00, so that the tenants received material regarding the rental conditions in the property they lived in.

On 22 December 2018, a resident contacted PrivatBo and informed them that the shared USB keys contained personal data.

On 23 December 2018, PrivatBo reported the relationship as a breach of personal data security to the Norwegian Data Protection Authority.

On 8 January 2019, PrivatBo sent a follow-up to the notification of 23 December 2018, including information on notification and handling in connection with the security breach. On 9 January 2019, the Danish Data Protection Authority received additional information by telephone regarding the actual circumstances surrounding the distribution of USB keys.

On 10 January 2019, the Danish Data Protection Authority sent a consultation letter with an accompanying questionnaire to PrivatBo.

On 12 and 13 January 2019, the Danish Data Protection Authority received two complaints that on 10 January 2019 PrivatBo had again handed out USB keys to the residents of the property "Svalegården". These USB keys contained a list of the leases in the property "Den Sønderjyske By". The list contained information about the address, the amount of the deposit and the amount of prepaid rent. In addition, the list indicated 17 cases where attachments had been made. Next to these leases was stated: "Disbursements made". In one case in addition, it was stated: "Loan deposit". On 28 May 2019, PrivatBo reported the security breach that took place on 10 January 2019 to the Danish Data Protection Authority. In a separate decision of 4 August 2020, the Danish Data Protection Authority seriously criticized the fact that PrivatBo inadvertently disclosed this information.

On 31 January 2019, the Danish Data Protection Authority received a report on the security breach that was reported on 23 December 2018. The report was prepared by Labora Legal on behalf of PrivatBo.

On 14 May 2019, the Norwegian Data Protection Authority requested PrivatBo for additional information about, among other things, who, in connection with the previous due diligence process, had been given the information that was on the three types of USB keys. On 31 May 2019, Labora Legal sent a supplementary statement on behalf of PrivatBo for use by the Danish Data Protection Authority in processing the case.

On 4 August 2020, the Danish Data Protection Authority notified PrivatBo to the Copenhagen Police and imposed a fine of DKK 150,000 for breaching Article 32 of the Data Protection Regulation in connection with the preparation and delivery of the USB keys that were delivered on 21 December 2018.

On 14 December 2020, however, the investigation was mistakenly discontinued and the criminal case closed by the police on the basis of a mix-up of several circumstances. The police have stated that the case cannot be reopened, as there is a turnaround time of 2 months according to the Administration of Justice Act. It has therefore not been possible to reopen the case.

2.2. Detailed description of the treatment

2.2.1. PrivatBo as data controller

It follows from Article 4, No. 7 of the Data Protection Regulation that "data controller" means a natural or legal person, a public authority, an institution or another body that, alone or together with others, decides for which purposes and with which aids personal data must be processed.

In its statement prepared by Labora Legal, PrivatBo has stated that PrivatBo considers itself the data controller in relation to data about tenants, as PrivatBo takes such an independent role in relation to tenants and landlords that PrivatBo itself decides which personal information is collected and for which purpose, which aids and decide the vast majority, if not all, of the case processing steps.

It is also the opinion of the Danish Data Protection Authority that PrivatBo, under the circumstances mentioned above, is the data controller.

2.2.2. PrivatBo's processing authority

Labora Legal has stated on behalf of PrivatBo that the disclosure of social security numbers and health information was

unintentional and due to an error.

It also appears from the statement that PrivatBo is of the opinion that it was not necessary to pass on the social security numbers and health information referred to in the case, and that there was therefore no authority for the passing on.

2.2.3. Technical and organizational security measures

In its report prepared by Labora Legal, PrivatBo has detailed the technical and organizational security measures that were implemented in connection with the provision of material for use in the obligation to offer and due diligence in order to ensure an appropriate level of security, taking into account the risks that the processing constituted.

Among other things, and in particular, PrivatBo has stated below that it carried out a personal data protection-based review of the documents where, regardless of the obligation to hand over the entire document, there could be an increased risk for data subjects.

It was identified that documents which there was a duty to hand over, but which could contain social security numbers, health information, information about criminal conditions and offences, as well as information which could obviously be required to avoid disclosure (information of a confidential nature), should be covered by the additional personal data protection-based review with a view to erasing the information or otherwise anonymizing the document.

PrivatBo has also stated that the review of the material was based on documents that could contain this kind of information. According to the instructions, the leases were not to contain information covered by the special review, and they were therefore not subject to the special personal data protection-based review.

PrivatBo has stated in the report that the reason why the leases were not the subject of the special personal data protection-based review was that, in connection with PrivatBo switching to digitization and scanning of the leases in 2003, an oral instruction was drawn up. The verbal instructions were a message to the employees that only the lease contract – and not other documents linked to the tenancy right – should be scanned. Social security numbers do not appear on the rental contracts themselves. Social security numbers and possibly personal data of a sensitive and confidential nature may, on the other hand, appear on other documents linked to the tenancy right.

According to the instructions, the drive on which the leases were stored should only contain the lease itself and no other documents. The lease contract for the individual lease had to be scanned as an independent PDF file, which also gave an overview of the fact that you had all the lease contracts.

In several cases, the underlying documents contrary to the instructions have nevertheless been scanned together with the lease. As a result of the fact that the instructions in connection with the scanning of rental contracts have not always been followed, social security numbers and a single piece of health information appeared in the material.

PrivatBo has stated in its statement that for documents covered by the incident, the scanning error occurred in 2006 (one document), 2013 (23 documents), 2015 (one document) and 2017 (five documents).

PrivatBo has also stated that, before sending the material, a random check was carried out to ensure that the files contained the correct documents, including specifically the lease.

It also appears from the statement that, taking into account the extensive amount of material that had to be reviewed, combined with the assessment of the likelihood that – contrary to established practice – there was a social security number and/or sensitive personal data associated with the lease, this became extensive, detailed and costly checks not carried out on every page of the document in the individual file with the lease. It was only checked that the file contained the lease (the first pages).

Furthermore, PrivatBo has stated that the material had been reviewed by the buyer and the buyer's advisers for a long period of time before it was handed over to the other residents, without it having given rise to any comments.

It appears from the statement that the risk assessment and the determination of the technical measures in connection with the handover pursuant to the obligation to offer were based on the misconception that the material did not contain special categories of information, cf. the data protection regulation's article 9 and did not contain personal identification numbers, cf. the data protection regulation's nature . 87, cf. § 11 of the Data Protection Act.

It is Privatbo's opinion that appropriate organizational measures have been laid down for the protection of personal information, cf. the data protection regulation, article 32, subsection 1. PrivatBo refers to the fact that it can be established that the organizational measures have resulted in the material not containing information about criminal convictions and offences, cf. Article 10 of the Data Protection Regulation, or that such information was pseudonymised, and that the material did not contain confidential personal data, cf. the Norwegian Data Protection Authority's description of this category at www.datatilsynet.dk.

Finally, it is Privatbo's opinion that the technical measures which were

appropriate, cf. the data protection regulation article 32, subsection 1, especially taking into account requirements for the release of a large number of personal data, which must be made "available" to residents pursuant to the obligation to offer, cf.

§ 100 of the Tenancy Act.

3. The Danish Data Protection Authority's assessment of the case

The Danish Data Protection Authority assumes that PrivatBo, under the provisions of section 2.1 mentioned circumstances, is the data controller.

The Danish Data Protection Authority also assumes that PrivatBo, in connection with due diligence and fulfillment of the duty to offer, cf. §§ 100-103 of the Tenancy Act, has inadvertently passed on a number of social security numbers and a single piece of health information.

Of the data protection regulation, article 32, subsection 1, it appears that the data controller must implement technical and organizational measures that suit the risks of varying probability and seriousness to the rights of the data subjects.

The data controller thus has a duty to identify the risks that the data controller's processing poses to the data subjects and to ensure that appropriate security measures are introduced to protect the data subjects from these risks.

The Danish Data Protection Authority is of the opinion that the requirements in Article 32 imply that PrivatBo has a duty to ensure that the personal data they process does not come to the knowledge of unauthorized parties.

Prior to the security breach, PrivatBo carried out a personal data protection-based review of the documents where, regardless of the obligation to hand over the entire document, there could be an increased risk for data subjects. Court book transcripts, decisions from the Rent Appeal Board and arrears lists have thus been anonymised.

PrivatBo has stated that the risk assessment and the determination of the technical measures in connection with the delivery pursuant to the obligation to offer were based on the delusion that the leases did not contain special categories of information. On this basis, the Data Protection Authority assumes that PrivatBo has relied on an oral instruction from 2003.

PrivatBo has referred to the extensive amount of material that had to be reviewed, together with the assessment of the likelihood that – contrary to the established practice – there was a social security number and/or personal data of a sensitive nature associated with the lease. On this basis, the Data Protection Authority assumes that PrivatBo has carried out a balancing of the workload by reviewing the material weighted against the risk for the registered.

The Danish Data Protection Authority finds that PrivatBo has not complied with its obligation, as data controller, to implement appropriate technical and organizational measures to ensure a sufficient level of security, which led to PrivatBo inadvertently passing on 39 social security numbers and health information in a virtual data room, to which 54 people had access in

connection with a due-diligence process, regardless of the fact that the social security numbers and health information were not necessary information in connection with fulfilling the obligation to offer according to §§ 100-103 of the Tenancy Act and the due-diligence process.

It is against this background that the Danish Data Protection Authority's assessment is that PrivatBo, in connection with the provision of material for use in the obligation to offer and due diligence, has not met the requirements of Article 32, subsection 1 of the Data Protection Regulation.

In the assessment, the Danish Data Protection Authority has emphasized that consideration of the workload by carrying out appropriate technical and organizational measures, including for example review of the entire material, does not - taking into account the specific risk assessment - exceed the consideration of securing the rights of the data subjects.

This is information that is passed on in connection with the obligation to offer and is therefore passed on to the registered persons' neighbours. There is therefore a risk for e.g. identity theft by unauthorized disclosure of the information. PrivatBo therefore has a responsibility to protect the tenants against these risks.

In addition, the disclosure of the information poses a risk of misuse of the information. In this connection, the supervisory authority has noted that it appears from PrivatBo's notification letter to the affected registered parties that PrivatBo cannot completely rule out the risk of misuse of personal information for, for example, identity theft and lending, and that PrivatBo therefore encourages the establishment of a credit warning in CPR.

In assessing that the security level was insufficient, the Danish Data Protection Authority has also emphasized that PrivatBo has relied on a very old oral instruction. Various employees have been responsible for the scanning, and it can be stated that the instructions have not been followed in several cases over a long period of years. A data controller must expect that not all employees follow the internal guidelines at all times. PrivatBo has not continuously checked that the instructions were actually followed and that no errors have occurred during the scanning.

After an overall assessment, the Danish Data Protection Authority is of the opinion that PrivatBo has not implemented appropriate technical measures to ensure a level of security that matches the risks to the rights of the data subjects, and that this is a serious violation of Article 32 of the Data Protection Regulation , subsection 1.

PrivatBo's reference to the fact that the material, which was provided for use in fulfilling the obligation to offer in connection with the due diligence process with the impartial buyer, had been reviewed by the buyer and the buyer's advisers, without it

having given rise to comments, cannot lead to another result.

The Danish Data Protection Authority must also note that the fact that the other party's lawyer has not alerted PrivatBo to PrivatBo's breach of the data protection legal rules cannot be considered a security measure in a data protection legal context.

The fact that PrivatBo has stated that spot checks were carried out to ensure that the files contained the correct leases cannot lead to a different result either.

In addition, the Danish Data Protection Authority must note that the purpose of the check was only to ensure that it was the correct file that was stored, and was neither intended nor suitable for ensuring that the document contained no other personal information than that which could be passed on. The random check cannot therefore be considered a sufficient security measure.

4. Summary

Based on the above, the Data Protection Authority finds that there are grounds for expressing serious criticism that PrivatBo A.m.b.A. of 1993's processing of personal data has not taken place in accordance with the rules in the data protection regulation, article 32, subsection 1.

[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).