

Decision regarding PrivatBo A.m.b.A. of 1993 in connection with breaches of personal data security

Date: 04-08-2020

Decision

Private companies

Journal number: 2019-441-1480

Summary

The Danish Data Protection Agency has found grounds for expressing serious criticism that PrivatBo - in connection with the obligation to make an offer - inadvertently handed over an overview of outstanding deposits and prepaid rent, and in some cases information about outlays in deposits, distributed to the tenants' address to residents in another property than that which was subject to the tender obligation in question. The unintentional disclosure of this information took place despite the fact that PrivatBo had hired an external auditing company in order to ensure the quality of the material.

Decision

Following an examination of the case, the Danish Data Protection Agency finds that PrivatBo's processing of personal data has not taken place in accordance with the rules in Article 32 of the Data Protection Regulation, and that with regard to the security breach that occurred on 10 January 2019, there is also a violation of Article 33.

The Danish Data Protection Agency has therefore today submitted a police report to the Copenhagen Police regarding the security breach reported on 23 December 2018.

In addition, the Danish Data Protection Agency finds grounds for expressing serious criticism that PrivatBo on 10 January 2019, as part of fulfillment of the obligation to make an offer, cf. information on outlays in deposits, distributed at the address of the leases to residents of a property other than that which was covered by the offer obligation in question.

In this connection, the Danish Data Protection Agency finds that PrivatBo, as data controller, has not implemented appropriate technical and organizational security measures to ensure an appropriate level of security, taking into account the risks posed by the processing and required by Article 32 of the Data Protection Regulation.

The Danish Data Protection Agency also finds grounds for expressing serious criticism that PrivatBo did not, in connection with the security breach that took place on 10 January 2019, without undue delay and within 72 hours after PrivatBo became aware of this, report the breach to the Danish Data Protection Agency, which constitutes a violation. Article 33 of the Data Protection

Regulation.

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

1. Case presentation

PrivatBo assisted in 2018 as part of the administration Frederiksberg Boligfond in connection with an intended sale of the properties "Peter Bangs Hus", "Svalegården" and "Den Sønderjyske By". In this connection, PrivatBo prepared material for the properties in question in connection with the tender obligation, cf. sections 100-103 of the Rent Act. The material was distributed to the tenants of the properties in question on USB keys.

On 23 December 2018, PrivatBo reported a breach of personal data security to the Danish Data Protection Agency, as PrivatBo in connection with a due diligence and fulfillment of an offer obligation, cf. sections 100-103 of the Tenancy Act, had inadvertently passed on a number of social security numbers and a single health information and on USB keys distributed to residents covered by the offer obligation.

On 8 January 2019, PrivatBo submitted a follow-up to the notification of 23 December 2018, including i.a. information on notification and handling in connection with the security breach.

On 10 January 2019, the Danish Data Protection Agency sent a consultation letter with an accompanying questionnaire to PrivatBo, which was asked to explain the security breach in more detail, including what technical and organizational measures had been implemented prior to the security breach.

On 12 and 13 January 2019, the Danish Data Protection Agency received two complaints that PrivatBo had again handed over USB keys to the residents of the property "Svalegården" on 10 January 2019. On the USB keys distributed to the tenants in the property "Svalegården" there was a list regarding the leases in the property "Den Sønderjyske By". The list contained information about address, amount of deposit and amount of prepaid rent. In addition, the list indicated 17 cases where outlays had been made. Next to these leases was stated: "Outlays made". In one additional case, it was stated: "Loan deposit".

On 31 January 2019, the Danish Data Protection Agency received a statement with accompanying appendices of the security breach, which was notified on 23 December 2018. The statement has been prepared by Labora Legal on behalf of PrivatBo.

On 19 February 2019, the Danish Data Protection Agency sent a consultation letter to PrivatBo, which was asked to explain the security breach in more detail on 10 January 2019. Labora Legal referred on behalf of PrivatBo in connection with the

statement of 31 January 2019.

On 14 May 2019, the Danish Data Protection Agency requested PrivatBo for further information, including the reason why the list was handed out to residents in "Svalegården".

On 28 May 2019, PrivatBo reported the security breach that took place on 10 January 2019 to the Danish Data Protection Agency.

On 31 May 2019, Labora Legal submitted a supplementary statement on behalf of PrivatBo for use by the Danish Data Protection Agency's processing of the case.

On 11 June 2019, the Danish Data Protection Agency requested PrivatBo for further information on e.g. the basis of the agreement with PwC, which was assumed as external quality control prior to the security breach that took place on 10 January 2019.

On 27 June 2019, Labora Legal submitted on behalf of PrivatBo a supplementary statement for use in the Danish Data Protection Agency's assessment of the security breach, which took place on 10 January 2019.

2. PrivatBos comments

2.1. The data controller processes

PrivatBo has in its statement prepared by Labora Legal, appendix 6, pkt. 3., stated that PrivatBo considers itself data responsible in relation to data on tenants, as PrivatBo plays such an independent role in relation to tenants and landlords that PrivatBo itself decides which personal information is collected and for what purpose, which aids and decide the vast majority, if not all casework steps.

2.2. Technical and organizational measures

In its statement of 31 January 2019 prepared by Labora Legal, appendix 6, PrivatBo has described in more detail the technical and organizational security measures that were implemented in connection with the provision of material for use in tendering and due diligence to ensure an appropriate level of security. taking into account the risks posed by the treatment.

Among other things, PrivatBo has stated, in particular, that a personal data protection-based review of the documents was carried out, 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 were required to be disclosed but which could contain social security numbers, health

information, information on criminal offenses and offenses as well as information that could obviously be required to be withheld (confidential information) should be included in the additional personal data protection review. to delete the information, or otherwise anonymize the document.

PrivatBo has further stated, partly in its statement of 31 January 2019 as Appendix 6 (PwC's own statement), partly in the statement of 31 May 2019, that PrivatBo, on the basis of the security breach notified on 23 December 2018, adopted PwC as external quality control to validate whether sensitive and confidential information was included in the material distributed on USB keys on January 10, 2019.

Finally, PrivatBo has referred to the fact that the list only contained reference to the lease number and address, and that it is therefore PrivatBo's opinion that this is pseudonymised information.

2.3. Notification of the security breach

On 19 February 2019, the Danish Data Protection Agency sent a consultation letter to PrivatBo, which was asked to explain the security breach on 10 January 2019.

In its statement of 31 May 2019, Labora Legal has stated that PrivatBo received notification on 10 January 2019 that the list in question had been handed over to the tenants in "Svalegården". PrivatBo immediately launched investigations and consulted with PwC, which stated that the list did not contain personal information.

Labora Legal has in its statement of 31 May 2019 stated that PrivatBo, on the basis of the Danish Data Protection Agency's latest inquiry (14 May 2019), has changed its view and acknowledged that the list contained personal data and that there has been a security breach. Against this background, PrivatBo reported the breach to the Danish Data Protection Agency on 28 May 2019.

Justification for the Danish Data Protection Agency's decision

3.1. Technical and organizational measures

The Danish Data Protection Agency assumes that PrivatBo, under the above in pkt. 2.1. mentioned circumstances, is the data controller.

The Danish Data Protection Agency also assumes that PrivatBo, as data controller on 10 January 2019, handed over a USB key with offer material to the tenants in the property "Svalegården", as part of the obligation to make an offer, cf. sections 100-103 of the Tenancy Act. error was a list on the USB key with personal information, which related to the tenants in the

property "Den Sønderjyske By", and that the disclosure of personal information was therefore unintentional.

Prior to the security breach, PrivatBo carried out a personal data protection-based review of the documents as a technical and organizational measure, where, regardless of the obligation to hand over the entire document, there could be an increased risk for data subjects. There has thus been anonymisation of court book transcripts, decisions from the Rent Appeals Board and arrears lists.

PrivatBo has also adopted PwC as an external quality control to validate whether sensitive and confidential information was included in the material, which was distributed on USB keys on 10 January 2019.

Article 32 (1) of the Data Protection Regulation 1, states that the data controller must implement technical and organizational measures that are appropriate to the risks of varying probability and severity of the data subjects' rights.

Thus, the data controller 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 put in place to protect the data subjects against these risks.

The Danish Data Protection Agency is of the opinion that the requirements in Article 32 imply that PrivatBo has a duty to ensure that the personal data which it processes does not come to the knowledge of unauthorized persons.

The Danish Data Protection Agency finds that PrivatBo, as data controller, has not implemented the appropriate technical and organizational security measures, in connection with the distribution of material for use in the tender obligation, to ensure an appropriate level of security, taking into account the risks posed by Article 32 of the Data Protection Regulation. .

In the assessment, the Danish Data Protection Agency has emphasized the nature of the breach, including the fact that it is a matter of passing on information on a list that is linked to an incorrect property. This is a mistake that is easy to detect without special expertise, and which is rooted in a lack of thoroughness. It is also emphasized that the security breach on 10 January 2019 is the second security breach in connection with the fulfillment of the tender obligation.

The Danish Data Protection Agency has also emphasized that the risk in passing on the information is the data subjects' reputation, including the assumption of poor finances.

The fact that PrivatBo has assumed PwC as external quality control and that PwC had indicated to PrivatBo that there was no personal data that was not necessary in connection with the fulfillment of the tender obligation, cannot lead to another result. In this connection, the Danish Data Protection Agency has emphasized that the error was easy to detect by inspection - also for persons without special professional knowledge.

However, the Danish Data Protection Agency has given weight in the mitigating direction that PrivatBo adopted PwC as external quality control.

The Danish Data Protection Agency must also note that the Authority does not agree with PrivatBo's assessment that the transferred personal data is pseudonymised, as the supplementary information does not meet the requirement in Article 4, no. 5, that it must be stored separately and be subject to technical and organizational measures. .

However, in assessing the breach of Article 32 in the mitigating direction, the Danish Data Protection Agency has emphasized that PrivatBo has generally been aware of data minimization.

Following an overall assessment, the Danish Data Protection Agency has found reason to express serious criticism of the matter.

3.2. Notification of the security breach

With regard to the notification of the security breach, the Danish Data Protection Agency assumes that PrivatBo already on 10 January 2019 became aware that the list had been handed over to the tenants in "Svalegården" by mistake. The Danish Data Protection Agency also assumes that PrivatBo was in an error, at least until 14 May 2019, that no personal data had been passed on.

Article 33 of the Data Protection Regulation states that breaches of personal data security, without undue delay and if possible within 72 hours after the data controller has become aware of the breach, must report it to the Danish Data Protection Agency, unless it is unlikely that the breach of personal data security poses a risk of the rights or freedoms of natural persons.

The Danish Data Protection Agency finds that there has been a violation of Article 33 (1). 1, as PrivatBo did not in connection with the security breach, which took place on 10 January 2019 without undue delay, and no later than 72 hours after PrivatBo became aware of this, reported the breach to the Danish Data Protection Agency.

In the assessment, the Danish Data Protection Agency has emphasized the time that has elapsed since PrivatBo became aware that a security breach had occurred until the breach was reported, and that PrivatBo has not proved that the breach of personal data security is unlikely to involve a risk to the rights or freedoms of natural persons.

The fact that LaboraLegal has stated that PrivatBo was for a period of time in an error as to whether it was personal data cannot, according to general principles of law and in particular in view of the fact that the error is not excusable, lead to a different result.

The Danish Data Protection Agency finds reason to express serious criticism of the situation.

In this assessment, the Danish Data Protection Agency has emphasized that this was the second security breach in connection with the tender obligation.