Supervision of IDdesign's processing of personal data

Date: 03-06-2019

Decision

Private companies

The Danish Data Protection Agency has reported IDdesign A / S to the police and set the company a fine of DKK 1.5 million for failure to delete information about approx. 385,000 customers.

Journal number 2018-41-0015

Summary

In the autumn of 2018, the Danish Data Protection Agency paid an inspection visit to IDdesign, where, among other things, was looked at whether the company had set deadlines for deleting customer information and whether the deadlines were complied with.

Prior to the audit visit, IDdesign had sent an overview of the systems that the company uses to process personal data. In this connection, IDdesign stated that in three independent, interacting IDEmøbler stores, an older system is still used, which has otherwise been replaced by a newer system in the other stores. IDdesign stated during the inspection visit that the old system processes information about approx. 385,000 customer name, address, phone number, email and purchase history.

IDdesign had not considered when personal data in the old system is no longer necessary for the purposes for which it is processed, and has thus not determined the deadlines that must apply to the deletion of the personal data processed in the system.

The Danish Data Protection Agency therefore finds that IDdesign has not complied with the Data Protection Ordinance's requirements for deletion, as the company has processed the personal data longer than necessary.

Decision

IDdesign was among the companies 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 Protection Authority's planned supervision of IDdesign focused in particular on the deletion of personal data in accordance with Article 5 (1) of the Data Protection Regulation. 1, letter e.

At the request of the Danish Data Protection Agency, before the inspection visit, IDdesign had filled in a questionnaire for each

of the systems selected by the Danish Data Protection Agency, in which personal data is processed, and submitted these together with additional material to the inspection. The actual inspection visit took place on October 8, 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 IDdesign has not complied with the requirements of Article 5 (1) of the Data Protection Regulation 1, letter e (storage restriction), as the company in the system AX 2.5 has processed personal data of approximately 385,000 customers for a longer period than necessary for the purposes for which they were processed.

That IDdesign has not complied with the requirements of Article 5 (1) of the Data Protection Regulation in relation to the information in system AX 2.5. Article 5 (2) 1, letter e, as the company has not set and documented deadlines for deletion of personal data.

That IDdesign has not complied with the requirements of Article 5 (1) of the Data Protection Regulation 1, letter e, as the company in the system AX 2012 has continued to process personal data about customers, after the company's own set deletion deadline for the information has been reached.

That IDdesign has not complied with the requirements of Article 5 (1) of the Data Protection Regulation in relation to the company's recruitment system and HR system. Article 5 (2) 1, letter e, as the company has not sufficiently documented its procedures for deleting personal data.

In relation to point 1, the Danish Data Protection Agency has today submitted a police report of IDdesign to the East Jutland Police. A copy of the police report is attached for information.

In addition, in relation to points 2-4, the Danish Data Protection Agency finds an overall basis for expressing serious criticism that IDdesign has not complied with the requirements of the Data Protection Ordinance.

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

Re point 1: Failure to delete personal data in AX 2.5

One of the systems in which IDdesign processes personal data is AX 2.5. The system is an ERP system [3], and it is the predecessor to AX 2012, which is now used by the company. AX 2.5 was phased out in the period March 21 to July 9, 2015.

IDdesign's current ERP system AX 2012 was - in contrast to AX 2.5 - one of the 7 systems that the Danish Data Protection Agency selected for review in connection with its inspection visit. This was partly due to the fact that IDdesign had informed the

Danish Data Protection Agency that IDdesign was the data processor - and not the data controller - with regard to the information in AX 2.5.

After the inspection visit, however, IDdesign has informed the Danish Data Protection Agency that the company is data responsible for the processing of personal data that takes place in AX 2.5 in connection with notices in invoices issued to IDdesign's customers in relation to customer cases / complaints and in the event of questions from SKAT.

In connection with the inspection visit, IDdesign has informed the Danish Data Protection Agency that information on customers' name, address, telephone number, e-mail and purchase history is processed in the AX 2.5 system.

Asked about AX 2.5, IDdesign stated during the inspection visit that the company has not set deletion deadlines for the personal data stored in AX 2.5, and has otherwise never deleted personal data in the system.

Finally, IDdesign has informed the Danish Data Protection Agency that the customer's telephone number is used as the customer ID, and in addition to the telephone number, the customer's name, address, e-mail and purchase history are stored.

IDdesign has also stated that at the time of the inspection visit, 823,178 "customer IDs" were stored in AX 2.5, and that the oldest personal information dates from 1 April 2010. According to IDdesign, the customer's telephone number is used as customer ID, and in addition to the telephone number, the customer's name, address, e-mail and purchase history are stored in connection with the customer ID.

Furthermore, IDdesign has subsequently explained the relevant customer IDs in AX 2.5. It appears that 430,100 customer IDs continue to be processed as a result of the legal obligation under section 10 of the Accounting Act, and that 448 other customer IDs are still processed, as customers still have a balance with IDdesign.

Finally, IDdesign has stated that the remaining 392,630 customer IDs have been deleted from AX 2.5 in the period from 12 December 2018 to 31 January 2019.

Since it is the customer's telephone number that is used as the customer ID, IDdesign has pointed out that duplicates may occur, which is why the actual number of registered persons will be slightly lower.

As the deletion of the 392,630 customer IDs had already been made when the Danish Data Protection Agency inquired about this, IDdesign could not state the exact number of duplicates. However, the company was able to state that among the 430,548 remaining customer IDs, 1.48% were duplicates, which means that information on 424,192 registered in AX 2.5 is still being processed.

The Danish Data Protection Agency then assumes that among the 392,630 deleted customer IDs, the percentage was the same number of duplicates, ie 1.48%, and the Authority therefore concludes that IDdesign kept information about approximately 385,000 previous customers' names, addresses, telephone numbers, e e-mail and purchase history, which is information about an identifiable natural person, cf. the nature of the Data Protection Regulation. 4 pieces. 1, No. 1.

The Danish Data Protection Agency is of the opinion that IDdesign's processing of customers' personal data in connection with the approximately 385,000 previous customer IDs is not in accordance with Article 5 (1) of the Data Protection Regulation. 1, letter e, which states that personal data must be stored in such a way that it is not possible to identify the data subjects for a longer period of time than is necessary for the purposes for which the personal data in question is processed.

It is noted in this connection that IDdesign itself has assessed that the information should be deleted from the system.

Re point 2: Lack of decision-making on and documentation of deletion deadlines in AX 2.5

Article 5 (1) of the Data Protection Regulation Article 5 (2) 1, letter e, it follows that the data controller must be able to demonstrate that it has not been possible to identify the data subjects for a longer period of time than is necessary for the purposes for which the personal data in question is processed.

As mentioned, IDdesign has stated that the company has not set deadlines for deletion of personal data in AX 2.5, and otherwise has never deleted personal data in the system.

Deciding when the collected and registered personal data is no longer necessary for the purposes for which they are processed, and thus when the data should be deleted from the systems, is the first and most basic step towards establishing correct and well-functioning procedures for deleting personal data.

It is therefore the Data Inspectorate's opinion that IDdesign has not complied with the requirements of Article 5 (1) of the Data Protection Regulation. Article 5 (2) 1, letter e, as IDdesign has not set and documented deadlines for deletion of personal data in AX 2.5.

Re point 3: Failure to delete personal data in AX 2012

Prior to the audit visit, IDdesign submitted a completed questionnaire regarding the company's processing of personal data in AX 2012, the new ERP system that IDdesign implemented in the period 21 March to 9 July 2015 as a replacement for AX 2.5.

The questionnaire states that personal information in AX 2012 is deleted depending on which category they are divided into.

As regards the category 'Customers', IDdesign has stated that information about the customers who have shopped at the

company in the form of their sales order, which also states their customer data.

IDdesign has stated that personal information in the category 'Customers' is anonymised after 912 days, corresponding to the right to make a complaint in 2 years. IDdesign has also noted that ½ years of extended complaint is offered in relation to the Purchase Act, and that there is a 25-year guarantee on some products, but that the deadline is set at 2½ years due to limitation of the processed personal data.

When asked about this, IDdesign stated in the questionnaire prior to the inspection visit that deletion of personal data in AX 2012, after the established deletion deadlines, takes place automatically in the system via batch jobs that are settled monthly.

During the inspection visit, the Danish Data Protection Agency wanted to investigate whether the deletion deadlines had been complied with in relation to processing customer information in AX 2012. In addition, IDdesign stated that the deletion procedures had not yet been implemented at the time of the inspection visit. There is information about customers in AX 2012 who had exceeded the deletion deadline of 912 days.

IDdesign has subsequently stated that the automated deletion procedure was implemented a few days after the inspection visit.

It is the opinion of the Danish Data Protection Agency that IDdesign - as the company has not complied with the deadlines for deletion of personal data about customers, which the company itself has set - has not complied with the requirements of Article 5 (1) of the Data Protection Regulation. 1, letter e, which states that personal data must be stored in such a way that it is not possible to identify the data subjects for a longer period of time than is necessary for the purposes for which the personal data in question is processed.

In its assessment, the Danish Data Protection Agency has emphasized that - on the basis that personal data has been entered in AX 2012 from no later than 9 July 2015 - this is a relatively short period of a maximum of 275 days, during which the information in question - at the time for the inspection visit on 8 October 2018 - had exceeded the deletion deadline of 912 days.

Re point 4: Lack of documentation of follow-up procedures for deletion in the YoungCRM and Timeplan systems

In connection with the inspection visit to IDdesign, the Danish Data Protection Agency has, among other things, reviewed procedures for deleting personal information in the company's recruitment system YoungCRM and the company's HR system Timeplan.

Prior to the inspection visit, IDdesign stated that deletion in the two systems is carried out manually on the basis of the established deletion deadlines.

During the inspection visit, the Data Inspectorate asked IDdesign how the company follows up that the deletions made in the systems have been carried out correctly and as expected.

As far as YoungCRM is concerned, IDdesign has stated that a monthly double check is made that there is no information that should have been deleted.

As far as Timeplan is concerned, IDdesign has stated that a corresponding double check is performed when deletions have been made in the system.

When asked about this, IDdesign has stated in relation to both YoungCRM and Timeplan that there are no written procedures for follow-up on deletion of personal data, but that these are fixed processes that must be entered in the existing procedures.

In order to meet its obligations under Article 5 (1) of the Data Protection Regulation Article 5 (2) 1, letter e, the data controller must establish and document procedures for follow-up that deletion of personal data has been carried out correctly and as expected.

It is therefore the Data Inspectorate's opinion that IDdesign has not complied with the requirements of Article 5 (1) of the Data Protection Regulation. Article 5 (2) 1, letter e, as IDdesign has not documented the company's procedures for follow-up on deletion of personal data in YoungCRM and Timeplan.

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 IDdesign has not complied with the requirements of Article 5 (1) of the Data Protection Regulation 1, letter e (storage restriction), as the company in the system AX 2.5 has processed personal data of up to 385,000 customers for a longer period than necessary for the purposes for which they were processed.

That IDdesign has not complied with the requirements of Article 5 (1) of the Data Protection Regulation in relation to the information in the AX 2.5 system. Article 5 (2) 1, letter e, as the company has not set and documented deadlines for deletion of personal data.

That IDdesign has not complied with the requirements of Article 5 (1) of the Data Protection Regulation 1, letter e, as the

company in the system AX 2012 has continued to process personal data about customers, after the company's own set deletion deadline for the information has been reached.

That IDdesign has not complied with the requirements of Article 5 (1) of the Data Protection Regulation in relation to the company's recruitment system and HR system. Article 5 (2) 1, letter e, as the company has not sufficiently documented its procedures for deleting personal data.

In relation to point 1, the Danish Data Protection Agency has today submitted a police report of IDdesign to the East Jutland Police.

In addition, in relation to points 2-4, the Danish Data Protection Agency finds an overall basis for expressing serious criticism that IDdesign has not complied with the requirements of the Data Protection Ordinance.

[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] An ERP (Enterprise Resource Planning) system is a system that brings together various processes such as purchasing and inventory management.