Disclosure of protected address information

Date: 26-02-2020

Decision

Private companies

The Danish Data Protection Agency expresses serious criticism of BEC's processing of personal data in connection with automatic transfers between banks.

Journal number: 2019-431-0044

Summary

The Danish Data Protection Agency has dealt with a case in which a number of banks and savings banks have reported that in connection with automatic money transfers between banks, personal information - including address information - was sent to persons who were registered in CPR with a protected or omitted address.

Due to the many reviews, the Danish Data Protection Agency decided to initiate an investigation of its own operations.

The banks' EDB Central (BEC) has stated that from the system that processed the automatic money transfers between banks, an advice was sent containing information about the payment sender, including information about his address. The system did not assess whether the address information was protected and therefore could not be disclosed. BEC has stated that more than 20,000 people have been affected by these transfers.

BEC has argued that conflicting rules - the money laundering rules on the one hand and the CPR Act on the other - have been a contributing factor to BEC not being able to unequivocally determine whether address information should be included in payment transactions or not.

Following the finding of the breach, BEC rectified the error in the transmission system, deleted the unauthorized transmitted address information and notified the data subjects concerned.

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

Decision

The Danish Data Protection Agency has become aware that in the period from 25 May 2018 to 22 August 2019, there have been a number of incidents related to the Banks' EDB Central A.M.B.A's (hereinafter BEC) IT system. The incidents have resulted in the unintentional disclosure of address information for persons who had address protection.

Decision

Following an examination of the case, the Danish Data Protection Agency finds that there are grounds for expressing serious criticism that BEC's processing of personal data has not taken place in accordance with the rules in Article 5 (1) of the Data Protection Regulation [1]. Article 32 (1) (f) and Article 32 (1) of the Data Protection Regulation 1.

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

2. Case presentation

The Danish Data Protection Agency has received a number of reports of breaches of personal data security from data controllers, cf. Article 33 of the Data Protection Regulation.

The Danish Data Protection Agency has, among other things, received notifications from Maj Bank A / S, Skandinaviska Enskilda Banken, Finansiel Stabilitet, Salling bank, Hvidbjerg Bank, Frøslev-Mollerup Sparekasse, BIL Danmark, Fynske Bank, Møns Bank, Merkur Andelskasse, Coop Bank A / S, Handelsbanken , PFA Bank, Lolland Bank A / S, Swedbank, Totalbanken, Vestjyske bank, Danske Andelskasse Bank, Frørup Andelskasse, Nykredit Bank A / S, Spar Nord Bank A / S, Faster Andelskasse, Andelskassen Fælleskassen, Lægernes Bank, Den Jyske Sparekasse and Arbejdernes Landsbank.

The notifications concern the disclosure of address information for persons registered with a protected address in the Central Person Register (CPR)

The address information is inadvertently passed on in connection with automated transfers between banks. It is estimated that more than 20,000 customers have been affected by the error.

It appears from the case that BEC is a data processor for a number of banks, some of which are co-owners, and thus member customers, and another part are service customers.

The data processing has taken place within the framework of concluded standardized data processing agreements.

A system error in a system that BEC has operated for the data controllers has resulted in a number of payment transfers (clearings) to payees at another bank at BEC or at other data centers having passed on address information about persons who in the CPR register is marked with address protection.

The following four different factors have been to blame for the incident:

there has been an older solution where no address protection has been implemented

in connection with the conversion of information from an older system to a new system, there has been an incorrect conversion

of a marking that controls the address protection

the marking of address protection - in connection with customers' updating of payments in the online bank - has been reset by mistake.

customers' choice to associate a so-called "special address" with their account, which is not checked for address protection in the system, has been mistakenly passed on during the transfer.

It appears from the case that BEC has corrected the error by making a number of patches in the system, and in addition has shielded the incorrect information for payees in BEC's online systems (online banking and mobile banking). On 3 September 2019, BEC deleted the historical entries from Danish banks and subsequently on 14 October 2019, deleted 2000 entries from foreign banks that could not be deleted in the first instance.

3. BEC's comments

By letter dated 27 December 2019, BEC has confirmed the facts stated.

BEC notes in its statement that sector agreements (Handbook for Sumclearing, Handbook for Intraday Clearing and Handbook for Immediate Clearing) state that payment transfers between two parties are usually accompanied by address information so that the payee can identify the payer. The sectoral agreements do not address the concept of address protection.

The sectoral agreements have been drawn up on the basis of rules for the transmission of information in payments, as set out in Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information to be transmitted in remittances. This Regulation does not deal with address protection.

Rules for processing protected addresses appear from LBK no. 646 of 02/06/2017

(CPR Act), i.a. § 28 on the establishment of address protection and § 44 on disclosure to other private individuals. The CPR Act mentions, for example, credit information agencies but does not express itself clearly about payment transactions and clearing.

However, BEC has assumed that it will be in accordance with the intention of the CPR Act that address information on persons with (name and) address protection is not passed on to payees in connection with payments, which has been unintentional in this case.

BEC further states that addresses, including protected addresses, will continue to be sent to foreign payment intermediaries, as these will otherwise be rejected in the receiving bank due to anti-money laundering and anti-terrorist financing controls.

BEC has carried out a systematic review of its systems and on that occasion made a number of patches. An internal system test in BEC showed on 22 October 2019 that in certain cases, when extracting entries via online banking, under certain conditions and preconditions, it was possible to include addresses for third-party transfers within the same bank - including protected addresses - in file extracts. . These are file extracts that are typically used by business customers for use in their internal financial systems.

BEC has handled this identified risk in relation to the specific data controllers concerned as an addition to the original incident and sent data to the data controllers for use in their specific risk assessment and further processing of the case.

BEC has stated that their systems have been running for many years. The payment transactions run in closed systems and there is no manual handling or control of the transactions, from the time they are initiated by a bank customer or a bank adviser, until they are received by the payee. A finding of the error has thus been due to the fact that a bank customer has approached his bank because he has suspected or established that a payee has received a protected address.

In general, BEC's systems have handled address protection since 18 September 2015. However, analyzes have shown that the functionality of a number of systems has not been implemented or has not worked as intended.

The handbooks that form the basis for payment transactions are prepared by Finans Danmark, and the handbooks have so far not mentioned the issue of address protection.

The development and testing of systems has therefore so far focused on requirements specifications arising from the sectoral agreements as well as Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015, where Article 4 (1) 1, states that the payer's address, official personal document number, customer ID number or date and place of birth must be enclosed by money transfers. Thus, the main focus has been on transaction flow. As address protection is not specifically mentioned in the said directive and sectoral agreements, matters concerning address protection have unfortunately not been addressed to the necessary extent.

This may be a contributing factor to the fact that there has not been sufficient attention and explicit requirement regarding address protection in payment transactions.

BEC has stated that address protection is activated by the citizen in the CPR register via the municipality of residence for a certain period at a time or permanently after an authority assessment.

BEC therefore only has access to information from CPR about currently protected addresses, and the time of the

establishment of the address protection. It is therefore not possible to calculate the number of historically affected data subjects accurately.

On 10 September 2019, BEC has, upon request to the CPR Office, been refused a request to receive historical CPR data on address protection from the Ministry of Social Affairs and the Interior with reference to section 38 of the CPR Act.

4. Justification for the Danish Data Protection Agency's decision

Based on BEC's own explanation, the Danish Data Protection Agency assumes that in this case BEC has unjustifiably passed on address information for persons to unauthorized persons, even though the persons were registered in CPR with a protected address, which was therefore not allowed to be passed on.

BEC has thus not sufficiently complied with the rules of Article 5 (1) of the Data Protection Regulation. 1, letter f.

Since BEC's systems have contained errors since 2015, which have resulted in customers' protected address information being passed on to unauthorized persons, BEC has not taken sufficient and appropriate technical or organizational measures, taking into account the current technical level, implementation costs and the nature of the processing in question. to ensure adequate security of the information in question, including protection against unauthorized or unlawful processing, and there has been no procedure for regularly testing, assessing and evaluating the effectiveness of these measures.

The Danish Data Protection Agency finds that BEC, by using an older IT solution where no address protection was implemented and that the conversion of personal data from an older system to a new system did not take place correctly and without control measures being established that could detect this, just as the marking of address protection - in connection with customers updating payments in the online bank - was accidentally reset and a number of customers' association of a default address to their accounts was not checked for address protection and therefore passed on, has not complied with the rules of the Data Protection Regulation 32, para. 1.

It is the opinion of the Danish Data Protection Agency that in connection with the processing of personal data, tests and ongoing follow-up must take place, which ensures that the personal data is processed with continued confidentiality, integrity, accessibility and robustness.

The Danish Data Protection Agency considers it aggravating circumstances that a very large number of customers' address information has been passed on, even though these were registered as protected in CPR and that the errors in BEC's systems have been present since 18 September 2015, without this being discovered.

In a mitigating direction, the Danish Data Protection Agency has emphasized that the conflicting rules in Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information - including address information - must be enclosed with money transfers and the rules on protected addresses in LBK no. 646 of 02/06/2017 (CPR Act), may be a contributing factor to BEC not being able to unambiguously determine whether address information should be included in payment transactions or not.

The Danish Data Protection Agency also emphasizes that BEC has quickly and efficiently - after the finding of the breach - brought the breach to an end and caused all the passed on addresses to be deleted.

Overall, the Danish Data Protection Agency must express serious criticism of the Banks' EDB Central A.M.B.A. for the violations that occurred.

[1] 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).