DATATILSYNET

Danske Bank A/S
Holmens Kanal 2-12
1092 København K
Danmark

Sent by Digital Post

3 June 2020

J.No. 2019-441-3337
Doc.no. 167462
Caseworker
[redacted]

The Danish Data Protection Agency
Borgergade 28, 5.
1300 Copenhagen
Denmark
T 3319 3200
dt@datatilsynet.dk
datatilsynet.dk

VAT No. 11883729

Personal data breach

The Danish Data Protection Agency (DPA) returns to the case where, on 13 September 2019, the DPA has received a data breach notification from Danske Bank A/S. The notification has the following reference number:

INC000002310272.

1. Decision

Following a review of the case, the Danish DPA finds that there are grounds to **reprimand** Danske Bank A/S, as the processing of personal data has not been done in accordance with the rules of Article 5(1)(f) and Article 32(1) of the General Data Protection Regulation (GDPR). The reprimand is issued in accordance with the rules of Article 58(2)(b).

The details of the case and the reasons for the decision of the Danish DPA are set out below.

2. Statement of facts

The data breach concerns District, an online financial platform for companies that are customers of Danske Bank, launched in January 2019.

In District, companies have an overview of accounts, transactions, available funds, etc. Furthermore, it is possible – by a written authority – to attach third parties to the District agreement, thereby gaining insight to e.g. accounts and transactions of said third parties. A third party can be another company, but can also be a data subject. A third party is always a customer of Danske Bank A/S.

The company using District can assign users – typically employees of the company – to access certain areas of District within the agreement between Danske Bank A/S and the company.

When a user must access information concerning a third party of a District agreement, a choice is made of the particular third party through a drop down menu. If the user has the proper access rights, the user will be able to access information on e.g. accounts and transactions concerning the third party. If the user does not have the proper access rights, the information will not be available.

The data breach consists in users within a District agreement, without the proper access rights, being able to see personal data – specifically name and social security numbers – of third party data subjects associated with the particular District agreement via the drop down menu, even

though the underlying information was not available. Danske Bank A/S has stated that this mistake has been present since the launch of District in January 2019.

Regarding the extent of the data breach, Danske Bank A/S has stated that it has not been possible to determine how many times data subjects' personal data was viewed wrongfully, due to the fact, that the data was accessible via a drop down menu. However, Danske Bank A/S has stated that only 12% of District users in Denmark have used the archive function through which the data was available.

As District is in use in Denmark, Sweden, Norway and Finland, data subjects in these member states are also affected by the data breach[1]. The following table provided by Danske Bank A/S outlines the number of data subjects potentially affected in each of the four member states, as well as the number of District users who had wrongful access.

	DK	SE	NO	FI
Total District agreements	33.958	17.742	8.945	36.409
Agreements containing third party data subjects	552	482	352	43
Data subjects (total)	8.913	539	1.723	2.204
Avg. data subjects per agreement	16	1	5	51
Users with wrongful access (total)	5.449	1.141	1.738	131
Avg. users with wrongful access per agreement	10	2	5	3

Danske Bank A/S has stated that the mistake in District – which allowed users to see names and social security numbers of third party data subjects, even though they did not have the proper access rights – was mitigated on 8 September 2019, 6 days after the breach was identified. The affected data subjects have not been notified of the breach.

Danske Bank A/S has stated that the affected data subjects will not be notified of the data breach as per Article 34, as there is no high risk to the rights and freedoms of data subjects. In this assessment, Danske Bank A/S has attached importance to the relationship between District agreement owners, third parties and data subjects, as well as the amount and types of data disclosed.

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

The Danish DPA considers that the data breach in District means that in 1.429 District agreements across Denmark, Sweden, Norway and Finland, 6 users on average had wrongful access to 9 data subjects' personal data.

According to Article 5(1)(f) of the GDPR, personal data must be processed confidentially, such that data cannot be accessed by anyone not authorized to do so. Furthermore, Article 32(1) states that the data controller must implement appropriate technological measures to ensure the confidentiality of personal data processed.

1 Danske Bank A/S has stated that District is also running as a pilot project in Northern Ireland, but that social security numbers were not available in this instance. Consequentially, Danske Bank A/S decided not to notify the Information Commissioner's Office (ICO). It is the opinion of the Danish DPA, that Danske Bank A/S' lack of notification to the ICO was justified.

It is the opinion of the Danish DPA that Danske Bank A/S should have ensured that only entries for those third parties, whom a District user is authorized to access, would appear in the drop down menu of the District archive.

On the basis of a review of the case, the Danish DPA finds that Danske Bank A/S' approach, under which – within a District agreement – information concerning all third party data subjects' names and social security numbers were made available to all users via the drop down menu, is not in conformity with Article 5(1)(f) and Article 32(1) of the GDPR.

Concerning Danske Bank A/S' decision not to notify the data subjects according to Article 34, the Danish DPA does not find itself in disagreement with the decision.

The Danish DPA has attached importance to the fact that it is technically feasible, with little effort, to populate the contents of the drop down menu in question with elements only concerning third parties of the District agreement, that the user rightfully has the authorization to access.

On the basis of the above, the Danish DPA finds that there are grounds to **reprimand** Danske Bank A/S, as the processing of personal data has not been done in accordance with the rules of Article 5(1)(f) and Article 32(1) of the General Data Protection Regulation (GDPR). The reprimand is issued in accordance with the rules of Article 58(2)(b).

4. Final remarks

The Danish DPA considers the case closed, and will not take further action in the matter.

Kind regards

[redacted]

Appendix:

- Legal basis

Extracts from Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons 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).

Article 5

Principles relating to processing of personal data

1. Personal data shall be:
   a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
   b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
   c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
   d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
   e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
   f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Article 32

Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
   a) the pseudonymisation and encryption of personal data;
   b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
   c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

e) In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

2. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

3. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.