DATATILSYNET

Dantherm A/S
Case register 298424

6 October 2021

J.No. 2020-441-6990
Doc.no. 399711
Caseworker
[redacted]

Notification of a personal data breach

The Danish Data Protection Agency
Carl Jacobsens Vej 35
2500 Valby
Denmark
T 3319 3200
dt@datatilsynet.dk
datatilsynet.dk

VAT No. 11883729

The Danish Data Protection Agency hereby returns to the case where Dantherm A/S (hereinafter Dantherm) has notified a personal data breach to the Danish Data Protection Agency on 25 September 2020. The notification has the following reference number:

c640f8bb456470f11b3bc3317e5594d2006d8bc3.

1. Decision

Following an examination of the case, the Danish Data Protection Agency considers that there are grounds for **issuing a reprimand** that Dantherm's processing of personal data has not been carried out in accordance with the rules laid down in Articles 32(1) and 24(1) of the GDPR, cf. Article 32(1).

Below is a detailed examination of the case and a statement of reasons for the Danish Data Protection Agency's decision.

2. Statement of the facts

On 25 September 2020, Dantherm notified a personal data breach to the Danish Data Protection Agency.

According to the notification, on the evening of 26 August 2020, Dantherm found abnormal behaviour on a backup server. Further investigation showed that on 21 August 2020 there had been malicious activity on the network. The activities had, according to the information provided, mainly concerned a study on network structure and destruction of running backups. At that time, the technical investigations carried out by the IT security company Dubex A/S (hereinafter Dubex) did not give grounds for suspecting a personal data breach.

The network connection was disconnected and the malicious activity was stopped. In cooperation with the hosting partners and Dubex, the network was opened with due care and further investigation of the hackers' behaviour on the network was launched.

In this context, it was found on 22 September 2020 at 21:00 that personal data from Dantherm had been exfiltered and posted online on a third-party hosting site. The data were confirmed to be removed on 23 September 2020 at 14.45.

In addition, it is apparent from the notification that the personal data concerned involved:

- bank details in the form of account details for salary payments of approximately 100-450 employees in Germany, Poland and England;
- Religious conditions exclusively for tax purposes of approximately 50 employees in Germany;
- Health data including in Denmark records of 87 health interviews and in Poland and England information relevant to the employment relationship;
- and personal identification numbers of approximately 1.525 citizens in Denmark.

On 15 June 2021, DAHL Lawyers delivered an opinion on behalf of Dantherm. DAHL stated, among other things, that on the basis of the activity that could be detected, Dantherm, in co-operation with Dubex, concluded that a ransomware attack had been launched against Dantherm, in which hackers had managed to access parts of the IT environment, but where the attack had not yet been carried out. At this point, the hacker and ransomware attack was averted.

The preliminary investigations showed no indication of a personal data breach, including the definitive deletion of data, the copying or distribution of data from Dantherm's IT environment, or the unauthorised access to personal data. This was only subsequently observed.

The further investigations led to the discovery on 22 September 2020 that personal data from Dantherm's IT environment was exfiltered in the form of one data file and that this data had been available from a server via a referral in a forum on the dark web. The file contained information on current and former employees.

On 23 September 2020, at 14.45, it was confirmed that the file had been removed online from the server where it was detected.

The studies carried out by Dubex indicated that the file was transmitted directly from Dantherm's IT environment to that hosting site. DAHL states in this regard that it has not been possible to investigate who, if any, has acquired the data while they have been online.

DAHL states that Dantherm had implemented a large number of security systems and that these were activated until the hackers partially deactivated some of them in connection with the attack. It is further apparent from the opinion of DAHL that Dantherm continuously deploys updates on servers in various rings via SCCM. There are various reasons why there are actually not always updates to the latest versions of operating systems immediately released. This is not generally considered to be contrary to best practice in the field, including that updates are not necessarily of a security nature.

DAHL has also stated that data has not been deleted at Dantherm and that Dantherm has not been denied access to data. Nor have the hackers made any claims for not publishing the data.

The data subjects concerned were informed by letters sent on 29 and 30 September 2020.

According to Dubex's report with conclusions on the cause of the breach, it was specifically one of the servers [redacted] that stood out as it had many services exposed to the internet, including Microsoft Remote Deskop (RDP). From this server it was subsequently possible to access other systems throughout the network to all internal systems. The attackers then turned off antivirus/malware and disabled event logging on all in the attack involved machines to avoid detection.

In addition, the Dubex report states that the attackers managed to log in to [redacted] server via the AD user account “AV”, which had previously been used by an external consultant in spring 2020 from an external company that had assisted Dantherm. Dubex has stated that “AV” was no longer with the external consultancy firm and there was therefore no reason for this account to log in to any of Dantherm’s systems. The account was a member of the domain administrator group and therefore had full access to all machines in the AD. According to Dubex, the attackers may have gained access to the account by guessing the password.

DAHL subsequently submitted on 20 July 2021 that Dubex informed Dantherm, when reporting the hacker attack, that the first account with administrator rights to which the hackers were given access was *probably* the user ‘AV’.

According to the report to Dantherm, it could not be demonstrated that the user “AV” had ever been logged on to the server [redacted]. In that regard, DAHL states that the conclusions are an indication of what is most likely and not an indication of what can be conclusively taken as established facts.

DAHL has also stated that Dantherm’s IT manager finds it just as likely that the hackers have accessed another domain administrator rights account as the first and only subsequently used the account “AV”, possibly because the hackers thought it was a service account for Dantherm’s antivirus system.

Finally, DAHL states that no actual answer can be given as to why the user account “AV” could still be used to log into Dantherm’s systems, as the hackers deleted most of the log files in the IT environment. The only thing that can be found is that the user account “AV” was not deleted. Whether the account was active or deactivated cannot be ascertained by Dantherm.

Dantherm’s normal procedure is that external consultants have access to the company’s IT systems only during the period each consultant has a real need to do so. When the individual consultant no longer needs access to Dantherm’s IT systems, the account is either deactivated or set to expire after a given date, and then deleted. When there is a presumption that after completing the specific task a consultant will perform tasks for Dantherm at a later stage, which requires access to the company’s IT systems, Dantherm typically does not delete the consultant’s account, but sets the account “disabled”. Under this status, the consultant cannot use the account to log in and access Dantherm’s IT systems.

In that regard, Dantherm’s IT manager states that it is the presumption that this normal procedure is also complied with in relation to the ‘AV’ account and that there are no indications that otherwise would be the case. As the relevant logs have been deleted by the hackers during the attack, Dantherm is unable to provide evidence of the circumstances in which the account “AV” has been active and during which periods the account has been deactivated. DAHL states in this regard that therefore it *cannot* be concluded that the account was active at the time of the attack.

In 2020, when the hacker attack took place, Dantherm’s IT department consisted of four employees with administrator rights. All four employees sat in the same office. Guidelines were therefore established and administered verbally in plenary session among these staff. Since the hacker attack, more employees have been added, and the current procedures are therefore being written down.

3. Reasons for the decision of the Danish Data Protection Agency

Based on the information in the case, the Data Protection Agency considers that Dantherm has been the victim of a hacker attack, which resulted in files containing information about employees being published on the dark web.

On this basis, the Danish Data Protection Agency finds that there has been unauthorised access to personal data, which is why the Danish Data Protection Agency considers that there has been a breach of personal data, cf. Article 4(12) of the GDPR.

According to Article 24(1) of the GDPR, a controller must implement appropriate technical and organisational measures to ensure and be able to demonstrate that the processing complies with the GDPR.

Article 32(1) of the GDPR states that the controller shall take appropriate technical and organisational measures to ensure a level of security appropriate to the risks posed by the processing of personal data by the controller.

There is thus an obligation on the controller to identify the risks that the controller's processing poses to data subjects and to ensure that appropriate safeguards are put in place to protect data subjects from those risks.

In the opinion of the Danish Data Protection Agency, the requirement for adequate security means that in system landscapes where access to confidential personal data or special categories of personal data can be created across different resources in the domain structure, there should normally be a limited administrative privileges. Therefore, it would normally be an expression of appropriate assurance that the administrator right is granted only to the relevant limited resources and for a limited period of time.

This could be done by not using broad administrative privileges and accesses and not granting them on a permanent basis, but only on an ad hoc basis.

The allocation of administrator rights should be organised in such a way that only relevant resources are accessed and, in all cases, machine registration (logging) of all uses of the rights is carried out. The logs shall also be stored in such a way that users with the administrative rights cannot delete or modify them.

In the light of the above, the Danish Data Protection Agency considers that, by failing to ensure that users with administrator rights could not delete or modify the log files, Dantherm has not taken appropriate technical measures to ensure a level of security appropriate to the risks posed by Dantherm's processing of personal data, cf. Article 32(1) of the GDPR.

The Data Protection Agency also finds that, by not being able to demonstrate during which periods the "AV" account was active, or by otherwise being able to clarify how the personal data breach occurred, Dantherm has failed to meet the requirement that the controller must be able to demonstrate adequate security in the processing of personal data, cf. Article 24(1) GDPR, cf. Article 32(1) GDPR.

Hereby, the Danish Data Protection Agency has emphasised that Dantherm has not sufficiently ensured the necessary documentation which, in the specific case, could clarify whether the GDPR was complied with.

Following an examination of the case, the Danish Data Protection Agency considers that there are grounds for **issuing a reprimand** that Dantherm's processing of personal data has not

been carried out in accordance with the rules laid down in Articles 32(1) and 24(1) of the GDPR, cf. Article 32(1).