DATATILSYNET

7 May 2024

The City of Copenhagen faces serious criticism for lack of security measures

The Danish Data Protection Agency has expressed serious criticism in a case where approximately 37,500 employees of the City of Copenhagen were granted unauthorised access to information on up to 3.7 million people – including sensitive information about children.

Summary

In connection with the transfer of files containing a large volume of data (disk swap), a human error resulted in overly broad user access being granted to the drive where the data was stored. This led to approximately 37,500 employees of the City of Copenhagen being granted unauthorised access to information on up to 3.7 million people. The data related to a so-called SAS installation (a format for management information, etc.), and only four SAS data warehouse developers were supposed to have had access to the data. For the majority of those affected, the data included, amongst other things, names and addresses; however, the files also contained information on well-being, language assessments and details regarding dental and healthcare for children.

This unrestricted access remained in place for just under two months, until the City of Copenhagen identified the error during a routine security scan of the municipality's open drives. Access was subsequently blocked, and the incident was reported to the Danish Data Protection Agency as a personal data breach.

In connection with the case, the City noted, however, that it was assessed that there was a very low probability of an ordinary IT user coming across the drive, as special knowledge was required to locate it. Network discovery was therefore disabled on the individual PCs, meaning that staff could not find the drive through normal searches on the PC. It also meant that the URL had to be known, or that the drive had to be actively scanned for. The local authority's investigations showed that no scanning tool had been used to search for open drives during the period of the breach. Furthermore, an examination of the administrative log revealed access only by individuals with a work-related need. However, the local authority's logs of all administrative IT users' potential access to the drive did not go back far enough in time for the local authority to conclusively determine that no employees other than those with a work-related need had accessed the information during that period. The local authority also stated that the majority of SAS files were not immediately readable by those who had gained unauthorised access to them, and that the data first had to be processed in a SAS programme.

Serious criticism of inadequate security measures

Following an overall assessment of the circumstances of the case, including the time that has elapsed since the incident, the Danish Data Protection Agency found grounds to express serious criticism of the fact that the City of Copenhagen's processing of personal data had not

been carried out in accordance with Article 32(1) of the General Data Protection Regulation concerning security of processing. The Danish Data Protection Agency therefore did not consider that the City had taken appropriate technical and organisational measures to ensure a level of security commensurate with the risks associated with the authority's processing of personal data.

In this regard, the Danish Data Protection Agency emphasised that the local authority had not ensured that only staff with a work-related need had access to the drive; that the system was set up in such a way that a single staff member's error could result in a breach affecting 3.7 million individuals, and that, immediately following the transfer of the data, no checks had been carried out to verify whether the access rights to the drive were correct – which would have immediately revealed the error, as all administrative staff had been granted access to it.

The Danish Data Protection Agency generally takes the view that, when developing new applications or moving file drives, an initial assessment must be made as to whether it is necessary, going forward, to move and store the data in a form that is personally identifiable. If this is necessary for the purpose of the processing, one possible security measure could be for the controller to ensure that the data is encrypted in such a way that only an authorised person can read and decrypt the data. A proprietary data format (such as a SAS format) cannot be equated with encryption, as there are often viewers or plug-ins that make it relatively easy to read the file formats in question.

Furthermore, for all development and maintenance tasks, it is essential that, as part of the change management process, a requirement is imposed that those authorised by the controller verify that the intended access control, monitoring and logging are functioning correctly before the change is released into production.

The Danish Data Protection Agency also noted in its decision that the municipality carried out periodic (quarterly) network scans for shared drives with the correct access rights, and that the municipality stated it would implement a number of measures to prevent a similar situation from arising again. However, the Danish Data Protection Agency also notes that the City of Copenhagen has subsequently reported several personal data breaches, consisting of employees gaining access to personal data which they had no work-related need to access, and that the Authority therefore expects the City of Copenhagen to maintain a continuous focus on ensuring that appropriate security measures are in place to reduce the risk of such breaches and to ensure that breaches are detected promptly.

Decision

The Danish Data Protection Agency hereby returns to the case in which the City of Copenhagen reported a personal data breach to the Danish Data Protection Agency on 17 June 2021.

1. Decision

Following an overall assessment of the circumstances of the case, including the time that has elapsed since the incident, the Danish Data Protection Agency finds that there are grounds for expressing serious criticism that the City of Copenhagen's processing of personal data has not been carried out in accordance with the provisions of Article 32(1) of the General Data Protection Regulation[1].

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

2. Statement of the case

On 17 June 2021, the City of Copenhagen reported a personal data breach to the Danish Data Protection Agency.

The Danish Data Protection Agency received a follow-up to the notification on 10 July 2021.

By letter dated 30 July 2021, the Danish Data Protection Agency requested further information regarding the case. Against this background, the City of Copenhagen submitted a statement on the case on 20 August 2021 (dated 13 August 2021).

It appears from the material submitted that, during a routine scan on 15 June 2021 of the City of Copenhagen's open file drives, it was discovered that a normally restricted drive containing data, including personal data, relating to an SAS installation[2] was accessible. Due to this error, it was possible for staff to search for and open the site in question. Access was blocked immediately after the error was detected.

It is further stated that investigations have shown that the breach was caused by human error, whereby an employee with administrator access inadvertently granted too broad access to the drive. It is believed that the error occurred in connection with data being moved to a larger disk on 17 April 2021.

The following information is provided regarding the data affected:

"The total number of individuals affected by the incident is a maximum of 3,750,000.

The affected E-drives contain, amongst other things, the following information:

- P-data: Address details – up to 3,750,000 CPR numbers.
- Information on pupils, including those who have left the school: approx. 504,000 CPR numbers
- Information on pupils' parents: approx. 480,000 CPR numbers
- Information on children in early years care, including those who have left the scheme: approx. 303,000 CPR numbers
- Information on the children's parents: approx. 120,000 CPR numbers
- Master data on staff: approx. 126,000 CPR numbers.

Please note – the figures above represent unique CPR numbers within each individual category of data – i.e. the numbers of CPR numbers cannot be added together. For example, the 504,000 pupils' CPR numbers are also included in the 'P-data Address Information' dataset."

It is further stated that, for the majority of the data subjects concerned, the information consists of name and address details; however, the files also contain information on the institution/school, family relationships for the group of children/parents in the municipality, and, in some cases, information on well-being, language assessment, and information on dental and healthcare services.

The City of Copenhagen has stated that access was too broad during the period from 19 April 2021 to 15 June 2021, and that no access was granted to individuals outside the City of Copenhagen.

During this period, the drive was accessible to all administrative IT users within the municipality. At the time the breach was detected, there were a total of approximately 37,500 administrative IT users in the City of Copenhagen.

Access should have been restricted to a single user group (AD security group) within the Children and Youth Administration. This user group grants access to a total of four SAS Data Warehouse developers in the Digitalisation and Data department of the Children and Youth Administration.

When the breach was detected, Group IT searched the administrative log, which goes back 35 days, for traces. The search revealed access only by specific, identified individuals with an authorised work-related need to access the server and the drive. However, the local authority's

logs of all administrative IT users' potential access to the drive do not go back far enough for the local authority to conclusively determine that no employees other than those with a work-related need accessed the server during that period.

The City of Copenhagen has stated that the likelihood of an ordinary administrative IT user within the municipality coming across the drive is very low, as it would require a regular user to have specific knowledge to locate the drive. In this connection, the City has stated that network discovery is disabled on individual PCs within the City. It cannot be enabled by an ordinary IT user without special access or permissions. This means that staff cannot locate the server via standard searches on their PCs. It also means that the URL must be known, or the drive must be actively scanned for. The Group IT security team periodically scans for open drives, as this is what an external attacker would do, and it was in this way that the broad access was identified. The URL is listed in the system's documentation, but finding it and copying it into File Explorer requires a deliberate intention to do so. The City of Copenhagen has therefore assessed that an ordinary IT user within the municipality would not have had the insight to locate the open server.

The City of Copenhagen has also demonstrated that no scanning tool was used to search for open drives during the period when broad access was available.

Furthermore, the City of Copenhagen has stated that only a very small proportion of the total data volume was available in plain text (0.2 per cent). The remainder of the data (99.8 per cent) consists of SAS files[3], which require the data to be processed in a SAS programme; this data was therefore not readable by a random administrative user at the City of Copenhagen. The City of Copenhagen has stated that the total volume of data, of which 0.2 per cent has been available in plain text, amounted to 1,827 gigabytes as at 10 August 2021. In this connection, the City of Copenhagen has noted that the volume of data changes daily as a result of ongoing data processing and updates.

The 0.2 per cent of the total data volume consisted of 8,424 files across the file types xsl, xlsx, xlsb and txt. The content of these files originates from a number of administrative and specialist systems and consists largely of school and institutional data and, to a lesser extent, information from the municipal paediatric dental care and health care specialist systems in the City of Copenhagen.

In this regard, the City of Copenhagen has stated that, for the data containing personal data, the majority will contain information about children.

However, part of the 0.2 per cent also comprises various types of aggregated report data and support data, such as organisational data used for management reporting.

The City of Copenhagen has stated that the data could be accessed via another SAS installation. In this context, the City has noted that its entire network infrastructure is monitored using the cyber security product 'Darktrace', which would have detected and raised an alarm had there been any attempt to retrieve these SAS files.

The following information is provided regarding the City of Copenhagen's measures prior to the incident:

- "Access control for the solution is managed via AD groups. Employees with a work-related need can thus be granted access to areas containing personal data at CPR number level through membership of one or more so-called AD security groups.
- Periodic (quarterly) network scans are carried out to check for shared drives with the correct access rights.
- Real-time network monitoring is carried out, with associated incident management, which, for example, detects the transfer of large amounts of data and unusual user behaviour.

- User instructions for data handling are available in the form of internal guidelines, and staff receive training.
- More standard technical measures include:
- Perimeter security in the form of firewalls and VPNs with two-factor authentication.
- Network isolation of servers, using both internal firewalls and microsegmentation.
- Access restrictions on servers in the form of access control lists.
- Centralised server log collection in a SIEM system."

The following information is provided regarding the City of Copenhagen's measures following the incident:

"Looking ahead, the City of Copenhagen has, amongst other things, implemented the following initiatives to prevent a similar situation from arising again:

- Ensured that logs are forwarded to the SIEM system in future (SIEM stands for Security Information & Event Management and is a collective term for a system that can collect logs from many different systems and is used to set up automated log monitoring) whenever server permissions are changed, so that precise changes can be traced and do not require interviews with staff.
- Instructions will be issued to all staff in the municipality's Group IT department stating that permissions on shares or drives must not be changed without a request from the system owner.
- A standard administrative procedure will be drawn up, setting out the rules and responsibilities relating to the creation of shares on servers. In line with this procedure, the Children and Youth Services Department will also instruct staff and external consultants that all changes to permissions on shares and drives must be created as requests in ServiceNow.
- The Children and Youth Administration will review the risk assessment for the processing of personal data on the server."

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

On the basis of the information provided by the City of Copenhagen, the Danish Data Protection Agency finds that, due to human error, an employee of the City of Copenhagen with administrator access granted overly broad access to a drive in connection with a disk swap on 17 April 2021, as a result of which all approximately 37,500 employees of the municipality gained unauthorised access to information on up to 3.7 million data subjects, including information on well-being, language assessments and information on dental and healthcare services relating to children.

On this basis, the Danish Data Protection Agency finds that there has been unauthorised access to personal data, and therefore considers that a personal data breach has occurred, cf. Article 4(12) of the General Data Protection Regulation.

3.1. Article 32 of the General Data Protection Regulation

It follows from Article 32(1) of the General Data Protection Regulation that the controller must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks associated with the controller's processing of personal data.

The controller is therefore under a duty to identify the risks that its processing poses to data subjects and to ensure that appropriate security measures are put in place to protect data subjects against these risks. As examples of relevant measures, the provision highlights, amongst other things, pseudonymisation and encryption, the ability to ensure ongoing confidentiality, and procedures for regularly testing, assessing and evaluating the effectiveness of the technical and organisational measures to ensure the security of processing, see Article 32(1)(a), (b) and (d).

It further follows from Article 32(2) that, when assessing the appropriate level of security, particular account must be taken of the risks posed by the processing, in particular by accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data that has been transmitted, stored or otherwise processed.

It is the Danish Data Protection Agency's view that the requirement under Article 32 regarding appropriate security will normally entail that, in systems containing a large amount of confidential information about a large number of users, higher standards must be set for the controller's diligence in ensuring, amongst other things, that there is no unauthorised access to personal data.

The City of Copenhagen's processing of personal data relating to up to 3.7 million individuals, including confidential and sensitive information, therefore places significant demands on the City's diligence in relation to, amongst other things, ensuring that there is no unauthorised access to the data. This applies, for example, to a processing activity where such personal data is stored on a drive, and where it must therefore be carried out in a manner that ensures that only staff with a work-related need have access to the data.

Furthermore, it is the Danish Data Protection Agency's view that the requirement for appropriate security will normally entail that, in the event of a subsequent change or transfer of data concerning a large number of data subjects, where a single human error could result in many employees gaining unauthorised access to the data, the controller must, immediately following such a change or transfer, test whether access rights are restricted to the relevant users and to the personal data necessary and relevant to those users' work-related needs; or, if access is more extensive, the controller must perform encryption of the personal data. It is therefore the Danish Data Protection Agency's view that, when carrying out disk swapping, the controller must implement measures to verify that the permissions on folders and files on the new disk are set identically to those on the previous disk.

In light of the above and following an overall assessment of the circumstances of the case, including the time that has elapsed since the incident, the Danish Data Protection Agency finds that there are grounds for expressing **serious criticism** of the fact that the City of Copenhagen's processing of personal data – by failing to ensure that only staff with a work-related need had access to the drive, by having a set-up where a single staff member's error could result in a breach affecting 3.7 million people, and by failing to test, immediately after the data was transferred, whether the access rights to the drive were correct – which would have immediately revealed the error, as all administrative staff had access – has not been carried out in accordance with Article 32(1) of the General Data Protection Regulation. Consequently, it is found that no appropriate technical and organisational measures have been taken to ensure a level of security appropriate to the risks associated with the authority's processing of personal data.

Furthermore, the Danish Data Protection Agency does not consider that the fact that most of the data (99.8 per cent) required an SAS installation to be readable could lead to a different assessment, as it is relatively easy to download an SAS installation from the internet and thus make use of the data. The Danish Data Protection Agency has noted that, according to the information provided, periodic (quarterly) network scans are carried out to check for shared drives with the correct access rights, and that it was precisely such a scan that enabled the City of Copenhagen itself to discover the breach, thereby limiting its duration to approximately two months. The Danish Data Protection Agency has also noted that the City of Copenhagen intended to implement a number of measures to prevent a similar situation from arising again. However, the Danish Data Protection Agency also notes that the City of Copenhagen has subsequently reported several personal data breaches, involving employees gaining access to personal data which they had no work-related need to access, and that the Authority therefore expects the City of Copenhagen to maintain a continuous focus on ensuring that appropriate security measures are in place to reduce the risk of such breaches and to ensure that potential breaches are detected promptly.

[1] 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).

[2] An SAS installation is a specialised format for management information and databases

[3] SAS files can also be read by anyone who has installed the correct software, which is available online, i.e. provided they have downloaded the correct 'viewer'.