The Danish Data Protection Authority expresses criticism and issues two orders to EG Digital Welfare ApS

Date: 07-07-2022

Decision

Private companies

Criticism

Injunction

Supervision / self-management case

Access control

Treatment safety

Password

Sensitive information

Logging

Social Security number

The Danish Data Protection Authority criticizes the data processor EG Digital Welfare ApS (EG) for not meeting the requirement for adequate security. The Authority also issues an order to carry out irreversible encryption of passwords and an order to secure login to special information.

Journal number: 2021-431-0144

Summary

The Danish Data Protection Authority has made a decision in an independent operation case regarding the IT system Mediconnect, which is offered by EG Digital Welfare ApS (EG). Mediconnect will, among other things, used by municipalities, regions and insurance companies to handle sensitive and confidential information about citizens. In this context, EG acts as a data processor for the Mediconnect IT system.

It appears from the case that passwords are stored in the Mediconnect IT system in clear text, and that information of special categories is only accessible by logging in with username and password.

Against this background, the Danish Data Protection Authority has expressed criticism of EG and issued an order to carry out an irreversible encryption of passwords, such that these are not found in the Mediconnect IT system in plain text. In addition,

the supervisory authority has given EG an order to ensure that the login solution, which gives access to personal data of special categories, does not take place solely by using a username and password.

Securing login to special categories of information

The decision states that it will not normally be adequate security to provide access to information of special categories only by entering a username and password when this is done over a network over which one has no control.

In continuation of this, the Danish Data Protection Authority is of the opinion that one-factor login entails an increased risk of misuse of access and the risk of access being shared by several users, such that any logging of access to the system is no longer effective, as one does not can be sure who actually used which accesses.

The Norwegian Data Protection Authority proposes that access be extended beyond username and password. This could be multi-factor login, use of certificates, tokens or a PKI solution.

Decision

In June 2021, the Danish Data Protection Authority received an inquiry that the Mediconnect IT system is used to handle thousands of cases and tens of thousands of documents with health information each year, and that the information is sent back and forth between municipalities, regions, insurance companies and specialist doctors through an insecure website. It also emerged from the inquiry that some accounts are used as joint accounts by several doctors and clinics. In addition, it appeared that two-factor login has not been introduced and that there is no machine registration (logging) of who accesses which information. It also emerged from the inquiry that passwords are available in plain text in the databases.

The Danish Data Protection Authority decided to investigate the matter further on its own initiative[1]. In this connection, the Danish Data Protection Authority requested on 15 March 2022 EG Danmark A/S (hereafter EG) for an opinion on the matter, including to answer a number of questions. On 4 April 2022, the EC sent an opinion in the case.

Among other things, it appears from the statement that the Mediconnect IT system was developed and owned by EG Digital Welfare ApS, which is a company owned by EG, and that EG replied to the Data Protection Authority's letter on behalf of EG Digital Welfare ApS. It also appears that EG Digital Welfare ApS is a data processor for Mediconnect.

The present decision thus concerns EG Digital Welfare ApS as data processor for the Mediconnect solution.

1. Decision

After a review of the case, the Danish Data Protection Authority finds that there is a basis for expressing criticism that EG

Digital Welfare ApS' (data processor for Mediconnect) processing of personal data has not taken place in accordance with the rules in the data protection regulation[2] article 32, subsection 1.

At the same time, the Danish Data Protection Authority finds grounds to notify EG Digital Welfare ApS of an order to use a recognized algorithm for irreversible encryption (e.g. hashing) of all passwords, so that these are not stored or made available in clear text. The supervisory authority also finds grounds to notify EG Digital Welfare ApS of an order to introduce a login solution for all users of Mediconnect with access to information of special categories, such that it is not possible to access this information only by using a username and password.

The order is announced in accordance with the data protection regulation, article 58, subsection 2, letter d.

The deadline for compliance with the order is 2 September 2022. The Danish Data Protection Authority must request to receive confirmation that the order has been complied with by the same date. According to the Data Protection Act[3] Section 41, subsection 2, no. 5, anyone who fails to comply with an order issued by the Danish Data Protection Authority pursuant to Article 58, subsection of the Data Protection Regulation shall be punished with a fine or imprisonment for up to 6 months. 2, letter d.

Before the same date, EG must inform the Danish Data Protection Authority about what measures EG Digital Welfare ApS is taking in connection with the order.

Below follows a closer review of the case and a rationale for the Data Protection Authority's decision.

2. Case presentation

On 4 April 2022, EG sent a statement in the case on behalf of EG Digital Welfare ApS.

It appears from the opinion that Mediconnect is used by municipalities, regions and insurance companies, and that Mediconnect generally supports two different processes, namely the provision of specialist doctor and psychologist statements as well as the process for supporting the design of rehabilitation plans between municipalities and regions.

It also appears that Mediconnect supports communication between the requester and a healthcare practitioner. The requester can create a case and send it out for tender to a number of healthcare professionals chosen by the requester, who will then receive an email stating that they have entered a bidding round for a case, after which they will be given the opportunity to submit an offer. The handlers who are involved in the tender case can only see the case description itself, which is formulated by the requester. The requester chooses which offer he/she wants to use and then sends the case files, including information

about the specific citizen or patient, to the healthcare practitioner who is assigned the case.

EG has informed the case that Mediconnect also supports a solution that the municipalities and regions use in their joint work on early retirement, flexible work and sickness benefit cases. In these cases, the municipalities can send case files to the regions, who log into Mediconnect and read the case through and have the option of writing notes on the case. According to EG, the parties each have their own agenda in Mediconnect, where they book cases into their joint meeting in connection with investigations. It appears from the statement that the municipality completes and completes their rehabilitation plan for citizens in Mediconnect, and that it is the municipalities that instruct EG Digital Welfare ApS when cases must be deleted.

EG has stated in the statement that Mediconnect constitutes a tool to support the customers' needs for obtaining statements and cooperation between municipalities, regions and insurance companies, in which connection EG Digital Welfare ApS acts as a data processor.

It also appears from the case that the individual healthcare professionals can register for the specialist database in Mediconnect if they wish to be able to bid on cases. To be created in the specialist database, the practitioner must fill in a form with contact details and their authorization ID. EG has stated that all specialists are checked by EG's support via postings in the authorization register before creation, and that all psychologists are asked to answer whether they are authorized or practicing psychologists, and that all therapists can ask to be deleted from the database at any time.

It also appears that general personal data is processed in Mediconnect in the form of information about name, address, e-mail address, telephone numbers, citizenship, birthday, gender, marital status, job title, employee ID, photos, etc., as well as confidential information about social security numbers and sensitive information about health conditions etc. EG has stated that the information processed concerns employees, citizens/patients and in some cases children and young people under 18 years of age.

EG has stated that EG Digital Welfare ApS offers all data controllers the opportunity to use ADFS integration for login management, but that not all existing customers have chosen to use the integration yet. EG has stated that EG Digital Welfare ApS has launched a campaign to get all data responsible requesters over to the ADFS solution, and that the option to use login via regular username/password will be completely shut down by the end of 2022 at the latest, just as the ADFS integration is a requirement for all new customers on Mediconnect.

It also appears from the case that the healthcare professionals are often smaller independent companies without the option of

using ADFS integration, which logs in via username and password. According to EG, the password must consist of at least eight characters and be an arbitrary combination of upper and lower case letters and numbers. EG has stated that if the practitioner enters the wrong code three times, their account will be locked, and that in order to log in again, they must use a function where they receive a code via their registered e-mail, which they must use in order to log in again the first time, after which they will be asked to create a new password.

EG has stated that EG Digital Welfare ApS has planned the rollout of two-factor login using SMS authentication for all health professionals from 1 October 2022 and it is expected that all practitioners will have switched to the new login method by the end of 2022.

EG has informed the case that EG Digital Welfare ApS logs everyone who accesses personal data in Mediconnect, including who, when and what that person has done, and that it is also logged who has accessed the audit log itself, which is on the database server.

It appears from the information in the case that EG Digital Welfare ApS only allows unique users and does not accept joint users, just as EG has stated that EG Digital Welfare ApS instructs all users not to use joint user logins in connection with teaching how to use the system.

EG has further informed the matter that as far as users who still use a username/password are concerned, the password is saved in clear text in the database. It also appears from the case that all passwords will be removed from the database for all users as they are moved to the multi-factor login method. EG has stated that only a very few selected EG employees with work-related needs have access to the database, and that all access is checked at least every six months.

3. Reason for the Data Protection Authority's decision

Based on what EG provided, the Danish Data Protection Authority assumes that Mediconnect does not require multi-factor login for users of the database. The Danish Data Protection Authority also assumes that passwords are stored in clear text in the database.

It follows from the data protection regulation article 32, subsection 1, that the data controller and the data processor must take appropriate technical and organizational measures to ensure a level of security appropriate to the risks involved in the processing of personal data.

The data processor thus has a duty to identify the risks that the processing poses to the data subjects and to ensure that

appropriate security measures are introduced to protect the data subjects against these risks.

The Danish Data Protection Authority is of the opinion that the requirement, cf. Article 32, for adequate security will normally mean that you, as a data processor and provider of a solution that provides access to information of special categories over a network over which you have no control, set the login system up so that it is only possible to log in using security in addition to username and password. This could be multi-factor login, use of certificates, tokens or a PKI solution. In addition to this, the Danish Data Protection Authority is of the opinion that one-factor login entails a risk of misuse of access and a risk of access being shared by several users, such that any logging of access to the system is no longer effective, as one cannot be sure who actually used which accesses.

Furthermore, the Danish Data Protection Authority is of the opinion that it would normally be an appropriate security measure to use a recognized algorithm for irreversible encryption (e.g. hashing) of all passwords, so that these are not stored or can be recovered in clear text. This applies regardless of which and how much personal data the processing includes. The background for this is that many registered users reuse passwords across services, etc., which is why there is an imminent risk that the password combined with e.g. an email address will be able to provide access to further information on other websites, etc.

Based on the above, the Danish Data Protection Authority finds that EG Digital Welfare ApS has not taken appropriate organizational and technical measures to ensure a security level that matches the risks involved in the company's processing of personal data, cf. the data protection regulation, article 32, subsection 1.

After a review of the case, the Danish Data Protection Authority finds that there is a basis for expressing criticism that EG Digital Welfare ApS' processing of personal data has not taken place in accordance with the rules in the data protection regulation, article 32, subsection 1.

When choosing a response, the Norwegian Data Protection Authority has emphasized that this is a system that has been developed for the processing of confidential and sensitive information about citizens, and that information about especially worthy of protection or weak persons, including minors, is also processed.

The Danish Data Protection Authority has noted that EG Digital Welfare ApS has planned to close down the possibility of using login via ordinary username/password by the end of 2022 at the latest, that ADFS integration is a requirement for all new customers on Mediconnect, and that all passwords will be removed from the database for all users as they are moved to the

multi-factor login method.

4. Injunction

After a review of the case, the Danish Data Protection Authority finds grounds to notify EG Digital Welfare ApS of an order to use a recognized algorithm for irreversible encryption (e.g. hashing) of all passwords, so that these are not stored or made available in clear text. The supervisory authority also finds grounds to notify EG Digital Welfare ApS of an order to introduce a login solution for all users of Mediconnect with access to information of special categories, such that it is not possible to access this information only by using a username and password.

The order is announced in accordance with the data protection regulation, article 58, subsection 2, letter d.

The deadline for compliance with the order is 2 September 2022. The Danish Data Protection Authority must request to receive confirmation that the order has been complied with by the same date. According to the Data Protection Act § 41, subsection 2, no. 5, anyone who fails to comply with an order issued by the Danish Data Protection Authority pursuant to Article 58, subsection of the Data Protection Regulation shall be punished with a fine or imprisonment for up to 6 months. 2, letter d.

[1] The Danish Data Protection Authority oversees any processing covered by the Data Protection Act, the Data Protection Regulation and other legislation that falls within the Data Protection Regulation's framework for special rules on the processing of personal data. The detailed rules can be found in Section 27 of 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 natural persons with regard to the processing of personal data and on the free exchange of such data and on the repeal of Directive 95/46/EC (general regulation on data protection).

[3] Act No. 502 of 23 May 2018 on supplementary provisions to the regulation on the protection of natural persons in connection with the processing of personal data and on the free exchange of such information (the Data Protection Act).