DATATILSYNET

MHI Vestas Offshore Wind A/S
Dusager 4
8200 Aarhus N

Sendt med Digital Post

27. januar 2021

J.No. 2019-441-3215
Doc.no. 258024
Caseworker
[redacted]

Notification of 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 thus returns to the case where MHI Vestas Offshore Wind A/S (hereinafter Vestas) submitted three notifications of breach of security to the Danish Data Protection Agency (DPA) on the 2nd of September 2019.

1. Decision

It appears from the case that Vestas, in connection with the launch of a new IT project to ensure a transparent and rigorous structure of accessrights in Vesta's ERP system, Microsoft Dynamics AX, discovered errors in the old structure.

2. Case presentation

The errors resulted in three personal data breaches, as three groups of employees had access to information about employees other than those they had an occupational need to have access too.

Thus, one group of employees has had access to general information about other employees without an occupational need for it. The information included the name, date of employment and termination of employment, details of seniority, private address, private telephone number, civil status of employees in England and Germany, ethnicity of five employees in England, date of birth, citizenship, language and 'corporate title'.

Another group of staff with personnel responsibility has had access to information on time records about employees not working under them. The information included name, number of hours recorded, the projects on which the employee had worked, and information on absenteeism, including unspecified sick leave.

In addition, a group of 176 people working with the handling of 'training certificates' had access to 'training certificates' of more employees than those they actually had a work-related need to have access to. The information referred to the name and qualifications.

The reason for the security breaches was a lack of structure in the access rights/rolls defined in Microsoft Dynamics AX.

2.1. Vestas Statement

Vestas has stated that risks to the rights and freedoms of the concerned individuals have been unauthorized access to their personal data by colleagues, which could lead to misuse of the data.

In this regard, Vestas has generally stated that Vestas does not have a specific suspicion that the employees who have had unintentional access to personal data have made use of this access, which the employees were not aware of. However, Vestas cannot verify this, as the system only logged if an activity was made, e.g. alteration or deletion of data, which did not happen. Vestas stated that only Vestas employees have had access to the data.

Vestas has also noted that the breaches were discovered at the start of an IT project on the 30th of August 2019 designed to improve the existing access rights structure of the company, which is why, at the time of the discovery of the breaches, a work plan and a budget had already been drawn up to make necessary changes to the structure. Vestas has also noted that the IT project, which has started up, is divided into two phases. The first phase concerns the rectification of the personal data breaches mentioned above. Vestas has stated that Vestas is not able to determine the exact time the breaches started, and as such cannot determine the duration of the breaches.

Regarding the first breach, Vestas has noted that the information on ethnicity was deleted when the company discovered that the data was stored, just as Vestas has limited the access to the employee information to those employees who have a work-related need to have access to the data.

Regarding the second breach, Vestas has noted that the time register is different for a "blue-collar" employee and for a "white-collar" employee, so the change in the structure of access rights is two-tier. Vestas has stated that as far as "blue-collar" workers are concerned, the problem has been solved. Vestas has also noted that the development of an amended "white-collar" system is in the design phase with a view to finding the best solution. Vestas has noted that the new solution has a high priority, which is why the company believes that it will be able to implement the solution within a short time span.

In relation to the third breach, Vestas has stated that access to training certificates has been restricted and the problem has therefore been resolved. Vestas has noted that training certificates are being transferred to another system where Vestas is in full control of the access rights structure. Migration would take place in the first quarter of 2020.

Regarding the second phase of the IT project, Vestas has stated that the company is carrying out a mapping of the access rights required by the employees in the various departments. This mapping will be compared to the current structure of access rights, according to which existing access rights can be verified and/or adjusted. Vestas observes that in doing so, the company can improve the structure in general and thereby provide information security.

Vestas has noted that another aspect of the second phase of the IT project is the implementation of a procedure whereby the IT department regularly publishes a list of individual employees' access rights to the department heads for their review.

Vestas has stated concerning the granting of access rights in the rights structure that it is built up in such a way that an employee is automatically assigned a number of minimum security roles. This is necessary for the employee to be created in the system. After this, the user is manually assigned the job roles (access rights) that the employee's boss has asked for IT to assign to the employee. Before assigning the requested job roles to the employee, IT makes an assessment of whether the proposed job roles are consistent with the rights normally granted to an employee in that department. In case a job role gives the employee access to personal data, the assignment must be approved by HR. In this regard, Vestas stated that it was not possible to mitigate the breaches by prior testing of the system, as the breaches occurred due to a human error to assign the correct access rights to the correct people.

Regarding the ongoing control of access rights, Vestas has noted that changes to an employee's access rights during the employment may take place on the basis of a request which is approved by his/her boss. In addition, Vestas has indicated that the IT department reviews the structure of access rights once every quarter to ensure that it is maintained. Vestas has also stated that external audits are organised twice a year. These are done by Ernest and Young.

3. Justification for Datatilsynets Decision

The Danish Data Protection Agency finds that the errors in assigning of access rights in Microsoft Dynamics AX have resulted in Vestas employees having unintentional access to information about other employees. Thus, The Danish Data Protection Agency finds that the errors that resulted in the breaches was due to human errors when assigning access rights in Microsoft Dynamics AX.

Article 32(1) of the Data Protection Regulation provides that the controller shall implement technical and organisational measures appropriate to the risks of varying probability and severity of data subjects' rights.

The Danish Data Protection Agency considers that the requirements of Article 32 imply that the controller has a duty to ensure that the personal data processed is not subject of unauthorized disclosure.

Following an examination of the case, the Danish Data Protection Agency considers that there are grounds for reprimand that Vesta's processing of personal data has not been carried out in accordance with the rules laid down in Article 32(1) of the Data Protection Regulation.

The Danish Data Protection Agency has put an emphasis on the fact that a number of employees had unauthorized access to information about other employees, including information of a confidential nature, that Vestas cannot verify if personal data of a confidential nature – including special categories of data covered by article 9 of the Data Protection Regulation – has been accessed, and that Vestas had not established procedures or tests – whether technical or organizational – that could have determined if the structure of the access rights were erroneous prior to the breaches, which also could have made Vestas aware of the duration of the breaches.

It is the opinion of the Danish Data Protection Agency, that it is of little importance to the assessment whether the personal data was indeed accessed, as the mere possibility of access to the personal data was an unnecessary risk to data subjects.

In assessing the appropriate response, the Danish Data Protection Agency has in a mitigating direction emphasized that Vestas has taken measures to ensure the restriction of access, including, inter alia, the development of new time registration systems, the development of procedures for continuous control of employees' access rights in the form of posting lists of job roles for review, and Vesta's organisation of internal as well as external audits.

4. Final Remarks

The Danish DPA hereby considers the case closed and will not take further actions in this case

Kind Regard

[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).

Section 2(1). This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

Section 32(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 ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

(2). 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.

(3). 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.

(4). 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.