UWV improves employer portal security after AP investigation

News item/June 4, 2020Category:

Security of personal dataMy sick employeeBenefit

After an investigation, the Dutch Data Protection Authority (AP) has determined that the Employee Insurance Agency (UWV) has improved the security of the online employer portal. The UWV has ensured that employers and occupational health and safety services can only log in to the portal via eHerkenning. The health data of employees stored in this system is thus sufficiently secured. The UWV therefore does not have to pay a penalty.

What preceded?

The AP concluded in 2017 that the security was insufficient and in 2018 imposed an order subject to periodic penalty payments on the UWV of 150,000 euros per month, with a maximum of 900,000 euros.

This was because the security level of the employer portal was not sufficient. The UWV did not apply multi-factor authentication when granting access to the employer portal.

Employers and health and safety services can use this portal to enter and view employee absenteeism data, among other things.

With the approaching deadline, the UWV indicated to the AP that many employers had not yet taken the step to eHerkenning. This created the risk that employees would not receive their sickness or maternity benefits on time.

Due to these possible negative consequences, the AP granted the UWV a one-off postponement until March 1, 2020, subject to conditions.

Absence data

Employers use the employer portal, among other things, to report sick and better employees. The UWV provides sickness benefits on the basis of these reports.

Various employee data is processed in the employer portal, such as name and address details, the BSN, financial data and data about incapacity for work, dismissal and childbirth.

Employers could log in to the portal via the internet by entering an email address and password. The AP concluded that the security of the portal was insufficient.

Multi-factor authentication

An organization that processes personal data must take appropriate measures to protect it properly. If the organization processes health data via the internet, extra strict requirements apply.

This is only allowed if users can only gain access if they have to use at least 2 authentication methods. For example with a password and an SMS code.