UWV improves employer portal security after AP investigation

News item/4 June 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 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 is therefore not required to pay a penalty.

What came before?

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

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

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

As the deadline approached, the UWV indicated to the AP that many employers had not yet made the move 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-time postponement until 1 March 2020 under certain conditions.

Absence data

Employers make use of 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 are processed in the employer portal, such as name and address details, the citizen service number (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 properly secure it. 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.