



DSGVO-Strafe in den Niederlanden ... bis zu EUR 900.000,-- für fehlende Mehr-Faktor-Authentifizierung

Mehr-Faktor-Authentifizierung beim Internetzugriff auf Gesundheitsdaten ist vorzusehen, sonst droht eine DSGVO-Strafe von bis zu EUR 900.000,--

Die [niederländische Datenschutzbehörde \(AP\)](#) verhängte eine DSGVO-Strafe, und zwar EUR 150T pro Monat mit einem Höchstbetrag von EUR 900T (dh für 6 Monate).

Es hat die staatliche "Agentur für Arbeitnehmersversicherung" (Uitvoeringsinstituut Werknemersverzekeringen (UWV)) getroffen, die Arbeitslosen- und Invaliditätsleistungen anbietet, und Arbeitssuchende vermittelt. Das ist mE mit dem Arbeitsmarktservice (in Ö) oder der Agentur für Arbeit (D) vergleichbar.

Die Strafe wurde mE "bedingt" verhängt, dh der Verantwortliche muss diese Strafe bezahlen, wenn er sein Portal nicht dem Sicherheitsniveau anpasst, dass die Aufsichtsbehörde als angemessen ansieht.

Die UWV bekam die Möglichkeit, das Sicherheitsniveau bis 31.10.2019 anzupassen, wobei diese Frist nun bis März 2020 verlängert wurde.

Aleid Wolfen, Vorsitzender des Aufsichtsbehörde:

*"Es geht um Gesundheitsdaten einer großen Anzahl von Menschen.
Alle diese Menschen müssen sich darauf verlassen können,
dass die UWV mit ihren Daten sorgsam umgeht."*

Gesundheitsdaten

Da die UWV beim Gewähren des Zugriffs auf das Online-Arbeitgeberportal **keine Mehr-Faktor-Authentifizierung** verwendet, aber ein **Zugriff auf Gesundheitsdaten** möglich ist, ist die Aufsichtsbehörde der Ansicht, dass **keine ausreichende Sicherheit** gewährleistet ist, da **keine Mehr-Faktor-Authentifizierung** verwendet wird.

Im Portal sind **Gesundheitsdaten für Arbeitgeber einsehbar**, da Krankenstandsdaten eingepflegt sowie eingesehen werden können. Die Entscheidung der Aufsichtsbehörde betrifft daher Gesundheitsdaten von Mitarbeiter*Innen. Als Anbieter und Betreiber dieses Systems zur Verwaltung der Abwesenheitsdaten ist die UWV verpflichtet, **den Zugang zu diesem Portal durch Anwendung einer Mindestauthentifizierung mit mehreren Faktoren sicher zu gestalten**.

Berechtigungskonzept / Absicherung vor unbefugten Zugriffen

Bei der Verarbeitung von personenbezogenen Daten hat der Verantwortliche geeignete Maßnahmen (siehe auch Art 32 DSGVO) zum Schutz derselben zu setzen. **Wenn Gesundheitsdaten verarbeitet werden, sind sehr hohe Anforderungen an die Datensicherheitsmaßnahmen zu stellen**.

Besteht die **Möglichkeit auf Gesundheitsdaten über das Internet zuzugreifen**, ist es nach Ansicht der Aufsichtsbehörde erforderlich, dass (mindestens) eine **Mehr-Faktor-Authentifizierung** verwendet wird.