THE
NATIONAL LAW REVIEW

Dutch Supervisory Authority Imposes GDPR Security Standard for Processing Broadly Defined Health Data

COVINGTON

Article By
Kristof Van Quathem
Covington & Burling LLP
Inside Privacy

- Communications, Media & Internet
- Global
- Health Law & Managed Care

- European Union
- Netherlands

Thursday, November 22, 2018

In early November, the Dutch Supervisory Authority released an injunction imposed against the public insurance body Uitvoeringsinstituut Werkgeversverzekering ("UWV") last July.

The UWV allows employers to submit data about their employees for social security purposes. The data includes dates of employee absences due to general illness (and when an employee is pregnant or gave birth, including dates of associated absences and parental leave). While the actual illness is not disclosed, the Supervisory Authority held that the data must be qualified as health data because the mere fact that someone is ill is indicative of their health.

In addition, the Supervisory Authority holds that the UWV violated the security standard of the GDPR by only applying one-factor authentication (e-mail address and password) on its portal. According to the Authority, state-of-the-art security for a platform with this level of risk requires multi-factor authentication. The Authority relies on Dutch guidelines for public authorities offering digital services and the Dutch NEN-7510 security standard for the health sector.

The UWV was ordered to conduct a new privacy impact assessment by October 1, 2018, and to implement appropriate security by October 31, 2019, with a penalty of €150,000 for each month delay (with a maximum of €900,000). The long transition period for improving its security is explained by delays in the roll-out of a standardized authentication tool for public bodies.

Source URL: https://www.natlawreview.com/article/dutch-supervisory-authority-imposes-gdpr-security-standard-processing-broadly