COLLEGE BESCHERMING PERSOONSGEGEVENS

POSTADRES Postbus 93374, 2509 AJ Den Haag BEZOEKADRES Juliana van Stolberglaan 4-10
TEL 070 - 88 88 500 FAX 070 - 88 88 501 INTERNET www.cbpweb.nl www.mijnprivacy.nl

AAN [Beheerder verzuimsysteem]

DATUM 2 juni 2015
ONS KENMERK z2015-00424
CONTACTPERSOON

UW BRIEF VAN
UW KENMERK

ONDERWERP De Wet bescherming persoonsgegevens en verzuimsystemen

Geachte directie,

Het College bescherming persoonsgegevens (CBP) voert regelmatig onderzoeken uit bij arbodienstverleners en werkgevers die in het kader van de verzuimbegeleiding gegevens over de gezondheid van werknemers verwerken in digitale verzuimsystemen.
Gegevens over iemands gezondheid zijn gevoelige gegevens. Voor het verwerken daarvan gelden extra wettelijke eisen. Werknemers bevinden zich in een kwetsbare positie omdat zij financieel afhankelijk zijn van de werkgever. Zij zijn verplicht om mee te werken aan hun re-integratie en moeten daarvoor alle benodigde medische informatie aan de bedrijfsarts verstrekken. Als deze medische gegevens niet zorgvuldig worden verwerkt, kan dat negatieve consequenties hebben voor de werknemers. Zorgvuldige omgang met medische gegevens staat dan ook hoog op de agenda van het College bescherming persoonsgegevens.

In de digitale verzuimsystemen treft het CBP herhaaldelijk verwerkingen van persoonsgegevens aan die in strijd zijn met het bepaalde in de Wet bescherming persoonsgegevens (Wbp). Ook ontvangt het CBP regelmatig vragen en signalen van verschillende partijen over de verwerkingen van gegevens over de gezondheid in verzuimsystemen.[1]

Met deze brief wil het CBP u daarom informeren over de beveiligingseisen die uit de Wbp voortvloeien en de manier waarop u aan deze eisen dient te voldoen.

**Beveiliging**
U, als bewerker/beheerder van een verzuimsysteem waarin gegevens over de gezondheid worden verwerkt, bent verantwoordelijk voor de beveiliging van dit systeem. Als de beveiliging van het systeem waar u verantwoordelijk voor bent niet voldoet aan de vereisten die voortvloeien uit artikel 13 Wbp, is er geen sprake van een zorgvuldige en behoorlijke verwerking van persoonsgegevens en handelt u daarmee in strijd met artikel 6 Wbp.

[1] https:/ / cbpweb.nl/ nl/ contact-met-het-cbp/ tip-ons

Uw systeem dient tenminste te voldoen aan de volgende concrete beveiligingsvereisten die voortvloeien uit artikel 13 Wbp:

- Indien het systeem wordt ontsloten via internet dient toegang tot het systeem door middel van tenminste tweefactor authenticatie te worden verkregen. Dit geldt voor alle gebruikers die toegang hebben tot het systeem;
- Beveiligingsrisico's dienen periodiek in kaart te worden gebracht, bijvoorbeeld door middel van penetratietesten en/of security scans. [2]

Zie voor een uitgebreid juridisch kader over de bovengenoemde aspecten van de beveiliging van verzuimsystemen door beheerders het rapport '*Onderzoek naar de beveiliging van Humannet Starter en Humannet Verzuim door VCD Humannet B.V.*'[3]

Ook overigens moeten passende organisatorische en/of technische maatregelen worden getroffen om beveiligingsrisico's te beperken danwel te voorkomen.[4] Onder passende technische en organisatorische maatregelen verstaat het CBP onder meer het volgende.

- De autorisaties van gebruikers dienen zodanig te worden ingesteld dat het niet mogelijk is dat personen die bepaalde medische gegevens niet mogen verwerken, deze gegevens toch kunnen inzien;
- De persoonsgegevens in de systemen mogen niet door de beheerder verwerkt worden ten behoeve van ontwikkeling en testen. Dit betekent dat voor ontwikkelen en testen gebruik dient te worden gemaakt van geanonimiseerde[5] of dummy gegevens.
- De werkgever mag bij de ziekmelding alleen die gegevens vragen die noodzakelijk zijn voor de begeleiding van de zieke werknemer. Dit zijn:
    - het telefoonnummer en (verpleeg)adres;
    - de vermoedelijke duur van het verzuim;
    - de lopende afspraken en werkzaamheden;
    - of de werknemer onder een van de vangnetbepalingen van de Ziektewet valt (niet onder welke);
    - of de ziekte verband houdt met een arbeidsongeval;
    - of er sprake is van een verkeersongeval met regresmogelijkheid.

  De overige gegevens (zoals bijvoorbeeld aard en oorzaak van de ziekte en medische behandelingen) mag de werkgever niet verwerken en registreren in het systeem. Dit betekent dat er geen (meerkeuze)mogelijkheden in het systeem mogen zitten die in strijd zijn met deze vereisten. Bij eventuele open invulvelden voor de werkgever moet duidelijk

[2] Zie Richtsnoeren beveiliging van persoonsgegevens van het CBP. https://cbpweb.nl/sites/default/files/downloads/rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf.
[3] Zie z2012-00288: Onderzoek naar de beveiliging van Humannet Starter en Humannet Verzuim door VCD Humannet B.V, december 2014, pag. 8 t/m 11.
[4] Zie Richtsnoeren beveiliging van persoonsgegevens van het CBP. https://cbpweb.nl/sites/default/files/downloads/rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf.
[5] Zie advies 5/2014 over anonimiseringstechnieken (WP 216) van de Groep gegevensbescherming artikel 29. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_nl.pdf.

zijn aangegeven dat hier geen medische gegevens in mogen wordt geregistreerd, zoals aard en oorzaak van de ziekte. Bij voorkeur worden er geen open velden in het systeem voor de werkgever aangeboden;
- Het moet voor de werkgever niet mogelijk zijn om rapportages uit te draaien waarin medische persoonsgegevens staan die niet door de werkgever verwerkt mogen worden.
- Als in opdracht van een werkgever de verzuimbegeleiding wordt uitgevoerd met behulp van een (zelfstandige) bedrijfsarts, mag de module waarin de arts de (medische) gegevens registreert op geen enkele manier toegankelijk zijn voor de werkgever, dus ook niet voor de systeembeheerder die in dienst is bij de werkgever.
- De uitgifte van inlogcodes voor de toegang tot gegevens die de werkgever niet mag verwerken, mag niet door de werkgever worden uitgevoerd. De uitgifte van deze inlogcodes impliceert namelijk dat de werkgever toegang heeft tot deze gegevens. De uitgifte van deze inlogcodes moet derhalve worden uitgevoerd door de beheerder van het systeem of de arbodienst.

**Handhaving**
Indien u een verzuimsysteem beheert dat niet voldoet aan de bovengenoemde vereisten, handelt u in strijd met de Wet bescherming persoonsgegevens. Het CBP verzoekt u in dat geval het verzuimsysteem zodanig aan te passen dat wordt voldaan aan de genoemde eisen die voortvloeien uit de Wet bescherming persoonsgegevens.
Het CBP zal zo nodig, op grond van tips of uit eigen beweging, onderzoek instellen naar de verwerking van persoonsgegevens in uw verzuimsysteem. Als uit onderzoek van het CBP blijkt dat uw systeem niet voldoet aan de vereisten die voortvloeien uit de Wet bescherming persoonsgegevens kan het CBP handhavende maatregelen inzetten.

Voor de goede orde merk ik op dat deze brief aan beheerders van verzuimsystemen ook (anoniem) op de website van het CBP (cbpweb.nl) is gepubliceerd en tevens is verzonden aan OVAL.

Hoogachtend,
Het College bescherming persoonsgegevens,
Voor het College,

Mr. W.B.M. Tomesen
Lid van het College