AUTORITEIT
PERSOONSGEGEVENS

<Onderzoeksrapport>

Werkgeversportaal UWV

Onderzoek naar het gebruik van meerfactorauthenticatie bij de toegang tot het werkgeversportaal van UWV

Rapport definitieve bevindingen
z2016-12305, augustus 2017

AUTORITEIT
PERSOONSGEGEVENS

Inhoudsopgave

1. Inleiding

1.1 Aanleiding onderzoek

In 2015 heeft de Autoriteit Persoonsgegevens (AP) publiciteit gegeven aan het onderwerp meerfactorauthenticatie, na afronding van een onderzoek naar een verzuimsysteem.[1] Authenticatie is het proces waarbij wordt nagegaan of een gebruiker, die in wil loggen in een applicatie/systeem, zich identificeert en aantoont dat hij/zij daadwerkelijk is wie hij/zij beweert te zijn. Het invoeren van een gebruikersnaam en wachtwoord is een voorbeeld waarbij de gebruikersnaam de identificatiefactor vormt en het wachtwoord een enkelvoudige authenticatiefactor is. Het invoeren van een gebruikersnaam, wachtwoord en een sms-code is een voorbeeld van meerfactorauthenticatie.
De AP heeft aan alle (bekende) beheerders van verzuimsystemen een brief gestuurd waarin is aangegeven dat toegang tot systemen waarin gegevens over de gezondheid worden verwerkt en die benaderbaar zijn via internet, door middel van tenminste tweefactorauthenticatie dient te worden verkregen. Dit geldt voor alle gebruikers die toegang hebben tot het systeem. De brief is ook op de website van de AP gepubliceerd.[2]

Enige tijd later heeft de AP een signaal ontvangen dat het Uitvoeringsinstituut Werknemersverzekeringen (UWV) gegevens verwerkt in een systeem (het werkgeversportaal) dat benaderbaar is via internet, waarbij geen gebruik wordt gemaakt van meerfactorauthenticatie bij het verkrijgen van toegang tot het systeem.

In het werkgeversportaal van het UWV worden onder andere gegevens over ziekmeldingen verwerkt van werknemers die tijdens ziekte door UWV betaald worden in het kader van de Ziektewet, bijvoorbeeld zwangere werknemers, uitzendkrachten en werknemers met een arbeidshandicap. Deze gegevens worden ingevoerd door werkgevers die via internet inloggen in het systeem.

Op grond van bovenstaande heeft de AP het UWV in een brief van 25 november 2015 gewezen op het feit dat toegang tot het werkgeversportaal via internet plaats moet vinden middels meerfactorauthenticatie indien er gegevens over de gezondheid in het systeem worden verwerkt.
Vervolgens is in de periode van 25 januari 2016 tot 24 februari 2017 meerdere keren contact geweest tussen de AP en het UWV. Het UWV heeft tijdens deze contacten aangegeven dat zij voornemens is om meerfactorauthenticatie in te voeren, maar hiermee te willen wachten tot zij gebruik kan maken van eHerkenning.

Op 27 maart 2017 heeft de AP een onderzoek als bedoeld in artikel 60 Wet bescherming persoonsgegevens (Wbp) ingesteld naar het gebruik van meerfactorauthenticatie in het werkgeversportaal van het UWV.

1.2 Het UWV

Het Uitvoeringsinstituut Werknemersverzekeringen staat in de Kamer van Koophandel ingeschreven onder nummer 34360247.

Het UWV zorgt voor de uitvoering van de werknemersverzekeringen, zoals de Werkloosheidswet (WW), de Wet werk en inkomen naar arbeidsvermogen (WIA), de Wet arbeidsongeschiktheid (WAO) en de Ziektewet (ZW). Daarnaast biedt het UWV arbeidsmarktdiensten, zoals arbeidsbemiddeling, re-integratie

[1] Autoriteit Persoonsgegevens: Onderzoek naar de beveiliging van Humannet Starter en Humannet Verzuim door VCD Humannet B.V, december 2014 (z2012-00288).
[2] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/brief_aan_beheerders_28052015_def_openbare_versie.pdf .

en gegevensdiensten. Het UWV voert deze diensten uit als zelfstandig bestuursorgaan (ZBO) in opdracht van het ministerie van Sociale Zaken en Werkgelegenheid.[3]

1.3 Het onderzoek

Doelstelling

Het doel van het onderzoek is na te gaan of het UWV passende maatregelen heeft getroffen, zoals bedoeld in artikel 13 Wbp ten aanzien van de authenticatie bij de toegang tot het werkgeversportaal via internet.

Hoofdvragen

1. Verwerkt UWV persoonsgegevens in het werkgeversportaal?
2. Zo ja, welke persoonsgegevens betreft dit?
3. Worden er gegevens over de gezondheid verwerkt in het werkgeversportaal van UWV?
4. Zo ja, is er sprake van passende beveiligingsmaatregelen, zoals bedoeld in artikel 13 Wbp, ten aanzien van de authenticatie bij de toegang via internet?

[3] Zie: https://www.uwv.nl/overuwv/wat-is-uwv/index.aspx.

2. Procedure

Naar aanleiding van een signaal heeft de AP het UWV in een brief van 25 november 2015 gewezen op het feit dat toegang tot het werkgeversportaal plaats moet vinden middels meerfactorauthenticatie indien er gegevens over de gezondheid in het systeem worden verwerkt.
Telefonisch heeft het UWV contact opgenomen over deze brief.
Bij brief, ontvangen op 25 januari 2016 heeft het UWV gereageerd op de brief van de AP.

Telefonisch heeft de AP op 1 maart 2016 contact opgenomen met het UWV met het verzoek een concrete planning aan te geven voor de invoering van meerfactorauthenticatie voor het werkgeversportaal.
Per e-mail van 7 maart 2016 heeft het UWV aangegeven dat zij geen concrete oplossingstermijn kan noemen.
Per e-mail van 15 maart 2016 heeft de AP nogmaals gevraagd een planning aan te leveren over de invoering van meerfactorauthenticatie.
Op 19 april 2016 heeft het UWV telefonisch contact opgenomen met de AP en aangegeven dat er niet meer informatie over de planning gegeven kan worden.

Bij brief van 21 juli 2016 heeft de AP middels een inlichtingenverzoek verzocht een concrete planning aan te leveren over de invoering van meerfactorauthenticatie voor het werkgeversportaal en een overzicht van maatregelen die het UWV heeft getroffen om de toegang van gebruikers tot het systeem zodanig te beveiligen dat wordt voldaan aan de vereisten die voortvloeien uit het bepaalde in artikel 13 Wbp.
Bij brief van 3 augustus 2016 heeft UWV de gevraagde inlichtingen verstrekt.
Bij e-mail van 9 augustus van 2016 heeft de AP nadere vragen gesteld over de informatie die wordt verwerkt in het werkgeversportaal.
Bij e-mail van 9 september 2016 heeft het UWV deze vragen beantwoord.

Op 21 november 2016 heeft telefonisch bestuurlijk overleg plaatsgevonden tussen de AP en het UWV.
Naar aanleiding hiervan heeft het UWV per e-mail van 30 november 2016, respectievelijk 9 december 2016 nog enkele vragen gesteld aan de AP. Telefonisch en per e-mail van 30 november 2016, respectievelijk 9 december 2016 heeft de AP hierop gereageerd.

Bij brief van 27 maart 2017 aan het UWV heeft de AP aangekondigd een ambtshalve onderzoek te zijn gestart naar de naleving van artikel 13 Wbp, in het bijzonder naar het gebruik van meerfactorauthenticatie bij de toegang tot het werkgeversportaal van het UWV.

Bij brief van 16 mei 2017 heeft de AP de voorlopige bevindingen van het onderzoek verzonden aan het UWV en ter kennisgeving aan de Minister die dit aangaat, te weten de Minister van Sociale Zaken en Werkgelegenheid.

Het UWV heeft op 23 mei telefonisch contact opgenomen om uitstel te vragen voor de indiening van de zienswijze. De AP heeft dit uitstel verleend.

Bij brief van 21 juni 2017 heeft het UWV een zienswijze gegeven op de voorlopige bevindingen.

Bij brief van 11 juli 2017 heeft de AP nadere vragen gesteld over de zienswijze. Op 14 juli 2017 heeft het UWV contact opgenomen met de AP om uitstel te vragen voor de beantwoording van enkele vragen. Op

uitnodiging van het UWV is de AP vervolgens op 18 juli 2017 bij het UWV ter plaatse gegaan om antwoord te krijgen op deze vragen, nadere vragen te stellen en inzage te verkrijgen in het werkgeversportaal.

Bij brief van 25 juli 2017 heeft het UWV de nadere vragen schriftelijk beantwoord.

3. Juridisch kader

3.1 Verwerking van persoonsgegevens

Volgens artikel 1, aanhef en onder a, van de Wbp wordt onder een 'persoonsgegeven' verstaan elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.

'Verwerking van persoonsgegevens' is gedefinieerd in artikel 1, aanhef en onder b, van de Wbp als "elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens."

3.2 Verantwoordelijke

Op grond van artikel 1, aanhef en onder d, van de Wbp is de verantwoordelijke de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

De wetsgeschiedenis geeft hierover aan: "Het begrip 'verantwoordelijke' knoopt in eerste instantie aan bij de vaststelling van het doel van de verwerking. De vraag is wie uiteindelijk bepaalt of er gegevens worden verwerkt en zo ja, welke verwerking, van welke persoonsgegevens en voor welk doel. Tevens is van belang wie beslist over de middelen voor die verwerking: de vraag op welke wijze de gegevensverwerking zal plaatsvinden. De richtlijn gaat ervan uit dat deze bevoegdheden in de regel in dezelfde hand liggen. Is dit niet het geval, dan is er sprake van gezamenlijke verantwoordelijkheid. [...]
Bij de beantwoording van de vraag wie de verantwoordelijke is, dient enerzijds te worden uitgegaan van de formeel-juridische bevoegdheid om doel en middelen van de gegevensverwerking vast te stellen, anderzijds – in aanvulling daarop – van een functionele inhoud van het begrip."

3.3 Bijzondere persoonsgegevens

De artikelen 16 t/m 24 van de Wbp gaan over de verwerking van bijzondere persoonsgegevens. In artikel 16 Wbp is bepaald dat gegevens over de gezondheid bijzondere persoonsgegevens zijn.

Gegevens over de gezondheid
Onder het begrip gezondheidsgegevens in de zin van artikel 16 Wbp vallen niet alleen gegevens waarop het medisch beroepsgeheim rust (zoals de aard, oorzaak en de behandeling van de ziekte) maar álle gegevens die de geestelijke of lichamelijke gezondheid van een persoon treffen.[4]

Dat het begrip "gezondheid" ruim moet worden opgevat wordt in de wetsgeschiedenis als volgt beschreven:
"*Het enkele gegeven dat iemand ziek is, is – conform de richtlijn – een gezondheidsgegeven in de zin van het wetsvoorstel, doch is geen medisch persoonsgegeven: zij omvat geen nadere informatie over de aard van de ziekte.*"[5]

[4] Autoriteit Persoonsgegevens, beleidsregels 'de zieke werknemer', februari 2015, pag. 10.
[5] Kamerstukken II 1997-1998, 25 892, nr. 3, pag. 102.

"[...] Het begrip 'gezondheid' moet niettemin ruim worden opgevat; het omvat niet alleen de gegevens die in het kader van een medisch onderzoek of een medische behandeling door een arts worden verwerkt, maar alle gegevens die de geestelijke of lichamelijke gezondheid van een persoon betreffen. Niet alleen indien een bedrijfsarts vaststelt dat een werknemer lijdt aan een psychosomatisch probleem is er sprake van een 'gegeven betreffende iemands gezondheid', dit is ook het geval indien een chef van een werknemer constateert dat de werknemer lichamelijk gehandicapt is."[6]

Ook de artikel 29-werkgroep (WP29) heeft advies gegeven over de term 'gezondheidsgegevens'.[7]
"The Working Party takes as a starting point that there is a category of information which is uniformly considered as health data. This is the category of medical data, the category of data about the physical or mental health status of a data subject that are generated in a professional, medical context. This includes all data related to contacts with individuals and their diagnosis and/or treatment by (professional) providers of health services, and any related information on diseases, disabilities, medical history and clinical treatment. This also includes any data generated by devices or apps, which are used in this context, irrespective of whether the devices are considered as 'medical devices'. But health data (or all data pertaining to the health status of a data subject) is a much broader term than the term 'medical'. Based on the current Data Protection Directive, national legislators, judges and DPA's have concluded that information such as the fact that a woman has broken her leg (Lindqvist), that a person is wearing glasses or contact lenses, data about a person's intellectual and emotional capacity (such as IQ), information about smoking and drinking habits, data on allergies disclosed to private entities (such as airlines) or to public bodies (such as schools); data on health conditions to be used in an emergency (for example information that a child taking part in a summer camp or similar event suffers from asthma); membership of an individual in a patient support group (e.g. cancer support group), Weight Watchers, Alcoholics Anonymous or other self-help and support groups with a health-related objective; and the mere mentioning of the fact that somebody is ill in an employment context are all data concerning the health of individual data subjects."

Geheimhoudingsplicht
In artikel 21, tweede lid Wbp is neergelegd dat op de verwerking van gegevens over de gezondheid een geheimhoudingsplicht rust.
"In de gevallen als bedoeld in het eerste lid worden de gegevens alleen verwerkt door personen die uit hoofde van ambt, beroep of wettelijk voorschrift, dan wel krachtens een overeenkomst tot geheimhouding zijn verplicht. Indien de verantwoordelijke gegevens persoonlijk verwerkt en op hem niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift een geheimhoudingsplicht rust, is hij verplicht tot geheimhouding van de gegevens, behoudens voorzover de wet hem tot mededeling verplicht of uit zijn taak de noodzaak voortvloeit dat de gegevens worden meegedeeld aan anderen die krachtens het eerste lid bevoegd zijn tot verwerking daarvan."

3.4 Beveiliging

Ingevolge artikel 13 van de Wbp dient een verantwoordelijke passende technische en organisatorische maatregelen ten uitvoer te brengen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Deze maatregelen moeten, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau garanderen gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen.

In het begrip 'passend' ligt besloten dat de beveiliging in overeenstemming is met de stand van de techniek.

[6] Kamerstukken II 1997-1998, 25 892, nr. 3, pag. 109.
[7] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf.

Het begrip 'passend' duidt mede op een proportionaliteit tussen beveiligingsmaatregelen en de aard van de te beschermen gegevens. Naarmate gegevens een gevoeliger karakter hebben, of de context waarin deze worden gebruikt een grotere bedreiging voor de persoonlijke levenssfeer betekenen, worden zwaardere eisen gesteld aan de beveiliging van deze gegevens.[8]

Gegevens over de gezondheid behoren tot de categorie bijzondere gegevens als bedoeld in artikel 16 Wbp. Dit betekent dat hoge eisen gesteld worden aan de technische en organisatorische maatregelen ter bescherming van deze gegevens.

Passende maatregelen
Om vast te stellen wat passende maatregelen zijn, zoals bedoeld in artikel 13 Wbp, gebruikt de Autoriteit Persoonsgegevens de beleidsregels 'Beveiliging van persoonsgegevens'[9] in samenhang met algemeen geaccepteerde beveiligingsstandaarden binnen de praktijk van de informatiebeveiliging, zoals de Code voor Informatiebeveiliging en de toepassing hiervan in de gezondheidszorg (NEN-7510).[10] Ook invulling van open normen door het Forum Standaardisatie en het College Standaardisatie worden door de AP gebruikt om vast te stellen wat passende maatregelen zijn, zoals in dit onderzoek het document 'Betrouwbaarheidsniveaus voor digitale dienstverlening'[11] en 'Betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten'.[12]

Passende maatregelen ten aanzien van authenticatie
Authenticatie is het proces waarbij wordt nagegaan of een gebruiker die in wil loggen in een applicatie/systeem zich identificeert en aantoont dat hij/zij daadwerkelijk is wie hij/zij beweert te zijn. Het invoeren van een gebruikersnaam en wachtwoord is een voorbeeld waarbij de gebruikersnaam de identificatiefactor vormt en het wachtwoord een enkelvoudige authenticatiefactor is. Het invoeren van een gebruikersnaam, wachtwoord en een sms-code is een voorbeeld van meerfactorauthenticatie.

Voorbeelden van normering ten aanzien van meerfactorauthenticatie vinden we onder meer terug in (A), de Code voor Informatiebeveiliging, (B) de NEN-7510 en (C) Betrouwbaarheidsniveaus voor digitale dienstverlening[13] en (D) Betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten.[14]

A: Code voor informatiebeveiliging.

[8] Autoriteit Persoonsgegevens: Beleidsregels beveiliging van persoonsgegevens, februari 2013, pag. 10 en Kamerstukken II 1997-1998, 25 892, nr. 3, pag. 99.
[9] Deze richtsnoeren zijn uitgebracht door het College Bescherming Persoonsgegevens, de voorloper van de Autoriteit Persoonsgegevens, en te vinden op URL: https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf
[10] NCSC, ICT-beveiligingsrichtlijnen voor webapplicaties, 31 augustus 2015, URL: https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html.
[11] Betrouwbaarheidsniveaus voor digitale dienstverlening, een handreiking voor overheidsorganisatie, Forum Standaardisatie, november 2016.
[12] Betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten, een handreiking voor overheidsorganisaties, Forum Standaardisatie, augustus 2014.
[13] Betrouwbaarheidsniveaus voor digitale dienstverlening, een handreiking voor overheidsorganisatie, Forum Standaardisatie, november 2016.
[14] Betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten, een handreiking voor overheidsorganisaties, Forum Standaardisatie, augustus 2014.

De belangrijkste normen voor informatiebeveiliging, ISO 27001 en ISO 27002 (hierna: Code voor Informatiebeveiliging) zijn recentelijk overgenomen als Europese normen.[15] Dit betekent dat beide normen in alle Europese landen als nationale norm worden gepubliceerd en conflicterende nationale normen worden ingetrokken.[16]
In de Code voor Informatiebeveiliging staat:
'*Om de geclaimde identiteit van een gebruiker te bewijzen behoort een passende authenticatietechniek te worden gekozen. Ingeval krachtige verificatie en authenticatie van de identiteit is vereist behoren andere authenticatiemethoden dan wachtwoorden te worden gebruikt, zoals cryptografische middelen, chipkaarten, tokens of biometrische middelen.*'[17]
en
'*De sterkte van gebruikersauthenticatie behoort passend te zijn voor de classificatie van de informatie waartoe toegang wordt verleend.*'[18]
en
'*Overwegingen betreffende informatiebeveiliging van elektronisch berichtenverkeer behoren de volgende aspecten te behelzen: [...]*
f) hogere niveaus van authenticatie voor het controleren van de toegang vanuit openbaar toegankelijke netwerken'[19].

B: NEN-7510.
De NEN-7510, die aanwijzingen geeft voor het toepassen van de Code voor informatiebeveiliging ISO/IEC 27002 in de gezondheidszorg, stelt de volgende eis:
"*Informatiesystemen, die patiëntgegevens verwerken, behoren authenticatie toe te passen op basis van ten minste twee afzonderlijke kenmerken.*"[20].

C: Betrouwbaarheidsniveaus voor digitale dienstverlening.
In betrouwbaarheidsniveaus voor digitale dienstverlening[21] wordt uitgewerkt hoe de betrouwbaarheidsniveaus dienen te worden bepaald, en wat dit onder andere betekent voor de authenticatie bij toegang tot de digitale dienst. Op een verwerking van gegevens waarop een bijzondere, wettelijk bepaalde, geheimhoudingsplicht rust en gegevens die onder het beroepsgeheim vallen in de zin van artikel 9, vierde lid van de Wbp is het betrouwbaarheidsniveau 'hoog' van toepassing. Op een verwerking van de overige bijzondere persoonsgegevens en op de verwerking van financiële gegevens is het niveau 'substantieel' van toepassing.[22]
Het betrouwbaarheidsniveau 'substantieel' betekent op grond van de Europese eIDAS[23] dat er sprake moet zijn van tweefactorauthenticatie.[24] Bij de toegang tot gegevens met het betrouwbaarheidsniveau 'hoog'

[15] De in het maatschappelijk verkeer bekend staande 'Code voor Informatiebeveiliging' bestaat uit twee delen: een norm (ISO 27001) en een 'code of practice' (ISO 27002).
[16] URL: https://www.nen.nl/NEN-Shop/ICTnieuwsberichten/ISO-27001-en-ISO-27002-voor-informatiebeveiliging-Europees-geadopteerd.htm.
[17] NEN IDO/IEC 27002:2013 + C1 + C2 nl, pag. 38. ISO 27002 is overgenomen als Europese norm. Dit betekent dat de norm in alle Europese landen als nationale norm wordt gepubliceerd en conflicterende nationale normen worden ingetrokken.
[18] NEN IDO/IEC 27002:2013 + C1 + C2 nl, pag. 38.
[19] NEN IDO/IEC 27002:2013 + C1 + C2 nl, pag. 69.
[20] NEN-7510 (2011), pag. 98.
[21] Betrouwbaarheidsniveaus voor digitale dienstverlening, een handreiking voor overheidsorganisatie, Forum Standaardisatie, november 2016.
[22] Betrouwbaarheidsniveaus voor digitale dienstverlening, een handreiking voor overheidsorganisatie, Forum Standaardisatie, november 2016, pag. 33.
[23] Vanaf 1 juli 2016 is de Europese eIDAS-verordening van kracht, waarin criteria zijn vastgelegd voor de betrouwbaarheidsniveaus van authenticatiemiddelen.

dient het middel goed beschermd te zijn tegen misbruik door anderen. "*Denk bijvoorbeeld aan een cryptografisch token, dat echter ook nog een PIN-code vereist, voordat het gebruikt kan worden. Deze PIN-code biedt een extra bescherming tegen misbruik door derden.*"[25]

D: Betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten.
In 'Betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten'[26] worden de verschillende niveaus van authenticatie uitgewerkt. Hierin wordt gesteld dat op een verwerking van gegevens waarop een bijzondere, wettelijk bepaalde, geheimhoudingsplicht rust en gegevens die onder het beroepsgeheim vallen in de zin van artikel 9, vierde lid van de Wbp het betrouwbaarheidsniveau 'hoog' van toepassing is. Op een verwerking van de overige bijzondere persoonsgegevens en op de verwerking van financiële gegevens is het niveau 'substantieel' van toepassing.[27]
Volgens het STORK-raamwerk[28] vereist het betrouwbaarheidsniveau substantieel "*striktere methoden voor de verificatie van de geclaimde identiteit van de gebruiker. Deze moeten een hoge mate van zekerheid bieden. […] Als type middel is 2-factor authenticatie vereist; gedacht kan worden aan 'soft' certificaten of one-time-passwords tokens.*"
Ten aanzien van het betrouwbaarheidsniveau hoog wordt geldt volgens het STORK-raamwerk: "*Dit niveau vereist tenminste eenmaal fysiek verschijnen van de gebruiker in het registratieproces en het voldoen aan alle eisen van de nationale wetgeving van het desbetreffende land aangaande uitgifte van gekwalificeerde certificaten als bedoeld in Annex II van Richtlijn 1999/93/EG betreffende elektronische handtekeningen. […]Dit systeem vereist gebruik van een token, een gewaarmerkt certificaat èn een digitale handtekening.*"

Conclusie passende maatregelen ten aanzien van authenticatie
Uit de bovengenoemde beveiligingsstandaarden vloeit voort dat ten aanzien van authenticatie bij de toegang tot applicaties waarin gegevens over de gezondheid worden verwerkt en waarbij toegang wordt verschaft via het internet, tenminste gebruik dient te worden gemaakt van meerfactorauthenticatie.

[24] Betrouwbaarheidsniveaus voor digitale dienstverlening, een handreiking voor overheidsorganisatie, Forum Standaardisatie, november 2016, pag. 24.
[25] Betrouwbaarheidsniveaus voor digitale dienstverlening, een handreiking voor overheidsorganisatie, Forum Standaardisatie, november 2016, pag. 25.
[26] Betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten, een handreiking voor overheidsorganisaties, Forum Standaardisatie, augustus 2014.
[27] Betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten, een handreiking voor overheidsorganisaties, Forum Standaardisatie, augustus 2014, pag. 22 en pag. 27.
[28] Dit raamwerk is in EU-verband ontwikkeld en vormt de 'ruggengraat' van het stelsel van betrouwbaarheidsniveaus waaraan enerzijds (families van) overheidsdiensten en anderzijds de beschikbare authenticatiemiddelen gekoppeld kunnen worden. Zie www.eid-stork.eu.

4. Feiten

4.1 Het werkgeversportaal

Op de website van het UWV staat over het werkgeversportaal:[29]
"Het UWV werkgeversportaal is de plek waar u alles regelt rondom werknemersverzekeringen.

Snel en makkelijk uw werknemer ziek of beter melden.
Re-integratieverslagen uploaden.
Ontslagaanvragen indienen.
Alle Ziektewet- en WAZO-brieven downloaden en opslaan.
Informatie voor eigenrisicodragers."

In de e-mail van 9 september 2016 van het UWV aan de AP stelt het UWV onder andere: "*Het werkgeverportaal is een platform met als doel om de digitale informatie-uitwisseling tussen UWV en werkgevers te faciliteren.*

- *Het portaal kent grofweg twee vormen van communicatie. Enerzijds kan het portaal als een soort postbus dienen. De door de werkgever gestuurde informatie wordt via het werkgeversportaal doorgeleid naar het juiste systeem. Dit geldt bijvoorbeeld voor de werkgeversstukken van het RIV en de ontslagaanvraag. Gemachtigden van werkgevers op het werkgeversportaal kunnen deze stukken na verzending niet meer inzien. Het kan ook andersom werken. UWV zet brieven aan werkgevers met beschikkingen digitaal klaar in het werkgeversportaal.*
- *Anderzijds biedt het portaal de functionaliteit om als platform te dienen. Werkgevers kunnen relevante informatie met UWV delen, hebben zelf inzage in deze informatie en kunnen in sommige gevallen wijzigingen aanbrengen. Dit geldt bijvoorbeeld voor de Verzuimmelder."*

4.2 Gegevensverwerking in het werkgeversportaal

In het werkgeversportaal worden onder meer de volgende gegevens verwerkt:[30]

- NAW-gegevens
- Brieven aan werkgever waaronder beschikkingen
- BSN
- Meetellen voor quotumregeling en/of banenafspraak
- Datum eerste AO-dag
- Datum laatste AO-dag
- Aard arbeidsverhouding
- Fase-indeling WFZ
- Loonbelastingtabel
- Indicatie loonheffingskorting
- Naam beroep ongecodeerd
- Percentage loondoorbetaling tijdens AO
- Bankrekeningnummer
- BIC - IBAN
- Woonwagenverwijzing
- Datum bevalling
- Datum gewenste ingang zwangerschapsverlof
- Datum vermoedelijke bevalling

[29] Zie: https://www.uwv.nl/werkgevers/werkgeversportaal/.
[30] Uit: Deze 'gegevensvelden' zijn afkomstig uit de bijlage in e-mail van 9 september 2016 van het UWV aan de AP.

- Bedrag SV loon gedeeltelijk werken eerste AO-dag
- Zwangerschaps-/bevallingsverlof
- Adoptieverlof
- Pleegzorgverlof
- Meerlingenverlof
- Bedrijfsongeval
- Ongeval door iemand buiten de werksituatie
- Zieke uitzendkracht
- Zieke oproepkracht
- Ziek uit dienst
- Ziek en valt onder no risk polis van de Ziektewet
- Ziek tgv zwangerschap
- Ziek tgv bevalling
- Ziek tgv orgaandonatie
- Samenloop met WIA
- Geen recht WIA en na wachttijd WIA niet werkzaam
- Samenloop met WAO of WAZ of 5 jaar voorafgaand
- Jonger dan 18 jaar en onderwijs belemmering
- Vanaf 18 jaar en onderwijs belemmering en geen WAJONG
- Recht op WAJONG-uitkering voorafgaande dienstbetrekking
- Ontvangst WAJONG-uitkering of ooit gehad
- Oordeel CWI functionele beperking
- Indicatiestelling WSW
- Arbeidsovereenkomst op grond van artikel 7 WSW
- Recht op voorziening t.b.v. arbeidsgeschiktheid
- Zwangerschapsverlof
- Verlengd bevallingsverlof
- Arbeidsongeschiktten gevolge van zwangerschap
- Overlijden
- Klachten ivm werkzaamheden
- Indicatie ontslag op staande voet

4.3 Toegepaste authenticatie in het werkgeversportaal

Op de website van het UWV staat ten aanzien van het inloggen op het werkgeversportaal het volgende.[31]
"Als u een account wilt aanvragen, ga dan naar uwv.nl/werkgeversportaal en klik op 'Een account aanvragen'. Uw account is gekoppeld aan uw e-mailadres. U kunt zelf een wachtwoord kiezen. U krijgt ter bevestiging van uw aanvraag een e-mail van UWV. Klik op de link in deze e-mail om uw accountaanvraag af te ronden. Met uw e-mailadres en wachtwoord kunt u voortaan inloggen."

De AP heeft op vier momenten contact opgenomen met het UWV over de toegepaste authenticatie in het werkgeversportaal.

Contactmoment 1
De AP heeft het UWV bij brief van 25 november 2015 gewezen op de norm dat dat toegang via internet tot een systeem waarin gegevens over de gezondheid worden verwerkt beveiligd dient te zijn middels meerfactorauthenticatie. In de brief van 25 januari 2016 stelt het UWV ten aanzien van de gebruikte authenticatie:
"*Ook wij hebben geconstateerd dat ons werkgeversportaal nog niet voldoet aan de beveiligingseisen die voortvloeien uit artikel 13 Wbp. De toegang tot het werkgeversportaal wordt inderdaad nog niet middels tweefactor-authenticatie verkregen. Dat is echter wel gewenst. De beveiligingsrisico's worden door UWV nu nog beperkt door het doen van penetratie- en securitytesten."*

Ten aanzien van de maatregelen die het UWV in dit kader treft stelt zij in dezelfde brief:
"Om bij het verlenen van toegang tot het werkgeversportaal toch een vorm van tweefactor-authenticatie te bieden doet UWV onderzoek naar het gebruik van de generieke (overheidsbrede) digitale voorziening e-herkenning. Dit om ons van een toekomstbestendige oplossing te verzekeren.
Het gebruik hiervoor door UWV stuit nu nog op het probleem dat in e-herkenning wel het KvK-nummer is opgenomen maar niet het RSIN (Rechtspersonen Samenwerkingsverbanden Informatie nummer). Het RSIN is voor UWV noodzakelijk om koppeling met andere gegevensbestanden mogelijk te maken.
Zodra het RSIN door de Rijksoverheid in e-herkenning is opgenomen zal UWV over kunnen gaan op deze voorziening, die dan tweefactor-authenticatie voor het werkgeversportaal gaat bieden."

Contactmoment 2
De AP heeft het UWV bij e-mail van 15 maart 2016 verzocht een concrete planning aan te geven voor de invoering van meerfactorauthenticatie.

UWV stelt hierop:[32]
"*Qua termijnen en het noemen van een termijn door UWV zijn wij, zoals in de brief staat vermeld, gebonden aan ontwikkeltermijnen van andere organisaties. We kunnen dus helaas geen concrete oplossingstermijn noemen.*
UWV kiest ervoor om binnen de generieke voorzieningen van het Rijk, i.c. e-Herkenning, te blijven en dus geen andere tussentijdse maatregelen te nemen die buiten het stelsel van Idensys vallen.
We zien het belang van het snel als onderdeel van de generieke voorzieningen van het Rijk beschikbaar komen van een betrouwbaar systeem van authenticatie. UWV probeert dit ook in de daarvoor bestemde gremia aan de orde te stellen.
UWV is derhalve met u van mening dat snelheid m.b.t. een oplossing geboden is. In de tussentijd verwachten wij met penetratie- en securitytesten de beveiligingsrisico's in beeld en onder controle te hebben.
Het treffen van aanvullende, nieuwe maatregelen zal een structurele oplossing door implementatie van het toekomstbestendige Idensys tenslotte mogelijk in de weg staan of in ieder geval vertragen."

[31] https://www.uwv.nl/werkgevers/faqwerkgeversportaal/account-en-machtigingen/detail/account-aanvragen, 28 maart 2017.
[32] E-mail van 7 april 2016 van het UWV aan de AP.

Contactmoment 3
Bij brief van 21 juli 2016 heeft de AP het UWV nogmaals gevraagd om een concrete planning voor de invoering van meerfactorauthenticatie en om een overzicht van de maatregelen die het UWV heeft getroffen om de toegang van gebruikers tot het werkgeversportaal zodanig te beveiligen dat wordt voldaan aan de vereisten die voortvloeien uit artikel 13 Wbp.

Bij brief van 3 augustus 2016 heeft het UWV de vragen beantwoord. In deze brief stelt het UWV nogmaals voornemens te zijn gebruik te gaan maken van eHerkenning. Daarbij tekent het UWV het volgende aan:
"*Om gebruik te kunnen maken van E-herkenning is het voor UWV noodzakelijk dat het gegeven RSIN (Rechtspersonen Samenwerkingsverbanden Informatie Nummer) wordt opgenomen. UWV maakt in zijn administratie gebruik van het RSIN nummer. Zonder dit nummer kan UWV E-herkenning niet koppelen aan zijn systemen (onder meer de Polisadministratie). Ook voor enkele andere overheidspartijen is koppeling aan RSIN noodzakelijk. Samen met deze partijen heeft UWV opname van het RSIN in E-herkenning als voorwaarde voor aansluiting gesteld. UWV stuurt bij diverse partijen aan op het aanleggen van de koppeling, onder meer bij de Kamer van Koophandel en bronhouder van het KvK-nummer en RSIN en bij het ministerie van Economische Zaken als initiatiefnemer van het stelsel E-herkenning. Door deze afhankelijkheid is het lastig om een concrete planning af te geven over dit proces, omdat besluitvorming in diverse gremia plaats moet vinden. Wij zien uw brief als extra steun om dit proces te versnellen. Na besluitvorming dient het RSIN binnen E-herkenning geïmplementeerd te worden. Pas daarna kan UWV overgaan tot feitelijk gebruik van E-herkenning en de daarmee tot toepassing van tweefactor authenticatie in het werkgeversportaal.*
Wij verwachten door onze afhankelijkheid van derde partijen dat ingebruikname van E-herkenning in 2018 te realiseren is. [...]"

Ten aanzien van de beveiliging van de toegang tot het systeem stelt UWV in die zelfde brief:
"*Wij zijn, met de Autoriteit Persoonsgegevens, van mening dat de gegevens binnen het werkgeversportaal in principe beveiligd moeten worden met tweefactor-authenticatie. Beveiliging met enkele authenticatie leidt tot extra risico's op verlies van gegevens, identiteitsfraude of onrechtmatige verwerking. [...]*
Omdat de implementatie van E-herkenning waarschijnlijk pas in 2018 rond zal zijn, is UWV tot dit tijd gebonden aan de huidige beveiliging met enkelvoudige authenticatie en beperkingen bij de uitvraag. De beveiliging ziet er momenteel als volgt uit:

- *Bij de registratieprocedure van een accounthouder op het werkgeversportaal, wordt een brief ter autorisatie aan de directie van het bedrijf gestuurd. Met gebruik van de code uit de brief, wordt een account geactiveerd. De directie dient akkoord te gaan met de voorwaarden van UWV en wordt daarmee bewust gemaakt van de verantwoordelijkheid voor het gebruik. UWV stelt strakke voorwaarden aan het door gebruikers te kiezen wachtwoord.*
- *UWV is in januari 2016 gestart met het uitvoeren van een BIRA (Business IB&P Requirements Analyse) om de beveiligingsrisico's van het werkgeversportaal inzichtelijk te maken. Momenteel wordt deze analyse afgerond waarna de verbeterpunten worden opgepakt. Daarnaast voert UWV Privacy Impact Assessments uit op het moment dat de gebruikte gegevens wijzigen ten gevolge van bijvoorbeeld wijzigende wetgeving. UWV voert bovendien jaarlijks penetratie- en securitytesten uit. Op basis van deze analyses vindt bijsturing plaats op de huidige beveiligingsmaatregelen.*
- *UWV voert op basis van specifiek patronen (use cases) continu logging van en monitoring op het gebruik uit. Dit is een geautomatiseerd proces. Hierbij wordt gekeken naar punten als meervoudige inlog met hetzelfde account vanaf hetzelfde IP adres, meerdere logins op meerdere accounts, meervoudige logins vanuit dezelfde locatie, bekende relaties tussen gebruikte IP adressen en account werkgever en inlog vanuit het buitenland. Als de systemen een signaal afgeven, wordt direct onderzoek ingesteld om eventueel misbruik zo spoedig mogelijk te*

beëindigen. Ook op anderszins naar voren komende signalen van misbruik, oneigenlijk gebruik of privacy schendingen wordt direct actie ondernomen.

- *Naast de specifieke maatregelen op het werkgeversportaal, gelden ook beveiligingsmaatregelen tegen hackers die op alle (webbased) systemen van UWV van toepassing zijn. Bijvoorbeeld bewaking met een Web Applicatie Firewall, een Intrusion Prevention Systeem en Anti-(D)DOS dienst.*

Er is dus sprake van een voortdurende controle op oneigenlijke toegang tot het werkgeversportaal en risicomanagement op de beveiliging.
Met deze maatregelen vindt UWV dat zij op een verantwoorde manier omgaat met het voorkomen van onbevoegde toegang tot de aan UWV verstrekte gegevens en dat UWV in lijn handelt met artikel 13 Wbp.
Wij houden bij onze beveiliging rekening met wat voor ons op dit punt en op dit moment mogelijk is, gegeven de stand van de techniek, de kosten en de risico's die UWV loopt. De door ons gewenste toepassing van E-herkenning is helaas nog niet beschikbaar, maar komt dat wel binnen afzienbare tijd. Het realiseren van een tijdelijke, alternatieve autorisatievoorziening (obv tweefactor authenticatie) zal eveneens de nodige tijd kosten en is vanuit een kosten-baten afweging niet wenselijk, noch voor UWV noch voor werkgevers."

Contactmoment 4
Op 21 november 2016 heeft telefonisch bestuurlijk overleg plaatsgevonden tussen een collegelid van de AP en de voorzitter van de Raad van Bestuur van het UWV.
In dit gesprek is gewezen op de verantwoordelijkheid van het UWV om zo snel mogelijk, te weten in 2017, te voldoen aan de vereisten die voortvloeien uit de Wbp.

Bij e-mail van 24 februari 2017 heeft het UWV laten weten dat niet zal worden overgegaan tot het invoeren van een tijdelijke voorziening voor tweefactor authenticatie.
"*UWV heeft op basis van het signaal van de AP de mogelijkheden onderzocht om in 2017 toch tweefactor authenticatie in te voeren via een tijdelijke voorziening. Hierbij is de SMS-service als meest haalbare oplossing geduid, onder meer omdat dit bekende technologie voor gebruikers is. Van de SMS-service is geanalyseerd wat de kosten, doorlooptijd en impact op de organisatie is. Uit de analyse blijkt dat invoering van een tijdelijke voorziening in 2017 feitelijk niet haalbaar is, rekening houdend met gangbare dienstverleningsnormen. Het is tevens ongewenst om UWV en werkgevers kort op elkaar een ingrijpend implementatietraject te laten doorlopen voor realisatie van tweefactor authenticatie.*"

Ten aanzien van eHerkenning stelt het UWV het volgende.
"*Inmiddels zijn vanuit de ontwikkelende partijen concrete toezeggingen ontvangen dat het RSIN nummer op korte termijn gekoppeld kan worden aan E-herkenning. Wij stellen voor om op korte termijn versneld te starten met de voorbereiding van de implementatie van E-herkenning. Realisatie is dan nog steeds in 2018. We kunnen na gedegen inventarisatie van de aansluitactiviteiten dit voorjaar een meer concrete planning afgeven.*"

Zienswijze op de voorlopige bevindingen
In de zienswijze van het UWV van 21 juni 2017 in reactie op het rapport voorlopige bevindingen van de AP stelt het UWV: "*Wij hebben naar aanleiding van uw brieven in december 2016 en januari 2017 onderzoek gedaan naar tijdelijke mogelijkheden meerfactorauthenticatie voor het werkgeversportaal. Uit dat onderzoek bleek dat een tijdelijke voorziening – ten opzichte van de implementatie van eHerkenning – een beperkte tijdwinst oplevert. Het is in onze ogen niet doelmatig en proportioneel om gelijktijdig twee implementatietrajecten te doorlopen die tweefactorauthenticatie bewerkstelligen. Dit leidt tot extra administratieve lasten voor werkgevers en ondoelmatige inzet van publieke middelen. Vandaar dat UWV in april 2017 heeft besloten de implementatie van de eHerkenning op te starten. Dit is mede mogelijk, omdat het technische knelpunt voor UWV rond de implementatie van eHerkenning – het identificeren van organisaties via het RSIN – sinds 1 juni jongstleden is weggenomen. Hiermee bewerkstelligen we onze ambitie om het beveiligingsniveau op onze portalen te verhogen naar niveau 'substantieel' waarmee we aan de door de Autoriteit*

Persoonsgegevens (AP) gestelde norm zullen voldoen. [...] Momenteel werkt UWV aan de eerste fase van de implementatie: het vooronderzoek. We verwachten in mei de aansluiting op eHerkenning gerealiseerd te hebben. Wij stellen voor in oktober 2017 te rapporteren over de voortgang van de implementatie van eHerkenning, eventueel in bestuurlijk overleg. Het vooronderzoek is dan afgerond. Wij zetten hiermee alle zeilen bij om eHerkenning zo snel mogelijk geïmplementeerd te hebben."

UWV stelt voorts in de zienswijze: "*gedurende de implementatie van eHerkenning willen we graag dat werkgevers gebruik kunnen blijven maken van onze portalen. De Wet bescherming persoonsgegevens (Wbp) verplicht UWV om een passend beveiligingsniveau te borgen gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen. We hechten daar zelf ook grote waarde aan. Wij achten het verantwoord om binnen het huidige beveiligingsbeleid te koersen op realisatie van tweefactorauthenticatie via de structurele overheidsbrede oplossing eHerkenning. Dit omdat wij het risico op inbreuk op de gezondheidsgegevens in ons werkgeversportaal laag achten, mede door de beveiligingsmaatregelen als geautomatiseerde monitoring op logging en penetratie- en securitytesten zoals ook verwoord in de voorlopige bevindingen op pagina 19. Dit wordt bevestigd in het uitgevoerde BIRA onderzoek door Noordbeek IT Audit, Compliance & Advisory. Wij blijven in onze verbetercycli streven naar verhoging van de beveiliging op ons portaal Er zijn ons op dit moment vanuit onze eigen beveiligingsteams of vanuit externe bronnen geen signalen bekend van misbruik van de genoemde gezondheidsgegevens.*
U adviseert op pagina 19 over andere maatregelen die genomen kunnen worden om de toegang tot de gegevens op het werkgeversportaal te beveiligen. Hierbij wordt een private VPN-verbinding genoemd. Wij hebben in de korte tijd voor deze zienswijze nog onvoldoende kunnen onderzoeken in hoeverre de implementatie van VPN mogelijk is en – tijdens de implementatietijd voor eHerkenning – kan bijdragen om de beveiliging van het werkgeversportaal te versterken conform norm van AP. Wij gaan uiteraard uw handreiking van het private VPN onderzoeken voor het op het wettelijk vereiste niveau krijgen van de beveiliging van ons werkgeversportaal. Wij stellen voor hierover in augustus 2017 te rapporteren. Mocht VPN niet realiseerbaar zijn, stellen we voor met u in gesprek te gaan over alternatieven."

5. Beoordeling

5.1 Verwerking van persoonsgegevens

Volgens artikel 1, aanhef en onder a, van de Wbp wordt onder een 'persoonsgegeven' verstaan: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.
'Verwerking van persoonsgegevens' is gedefinieerd in artikel 1, aanhef en onder b, van de Wbp en betreft elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens. Hieronder valt in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.

Het UWV verwerkt verschillende gegevens van personen in het werkgeversportaal. Het betreft onder andere NAW-gegevens, BSN, financiële gegevens en gegevens over arbeidsongeschiktheid, ontslag, en bevalling.[33]

Omdat de naam en het BSN van de personen onderdeel uitmaakt van de bovengenoemde gegevensset, hebben al deze gegevens betrekking op geïdentificeerde natuurlijke personen, te weten de personen waarvan gegevens worden geregistreerd in het werkgeversportaal. Bovengenoemde gegevens zijn derhalve persoonsgegevens als bedoeld in artikel 1, onder a, Wbp.

5.2 Verantwoordelijke

Op grond van artikel 1, aanhef en onder d, van de Wbp is de verantwoordelijke de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of te zamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

In de brief van 25 januari 2016 stelt het UWV: "*Ook wij hebben geconstateerd dat ons werkgeversportaal nog niet voldoet aan de beveiligingseisen die voortvloeien uit artikel 13 Wbp.*

Op de website van het UWV staat over het werkgeversportaal:
"*Het UWV werkgeversportaal is de plek waar u alles regelt rondom werknemersverzekeringen.*
Snel en makkelijk uw werknemer ziek of beter melden.
Re-integratieverslagen uploaden.
Ontslagaanvragen indienen.
Alle Ziektewet- en WAZO-brieven downloaden en opslaan.
Informatie voor eigenrisicodragers."

In de e-mail van 9 september 2016 van het UWV aan de AP stelt het UWV onder andere: "*Het werkgeverportaal is een platform met als doel om de digitale informatie-uitwisseling tussen UWV en werkgevers te faciliteren.*

Uit bovenstaande blijkt dat het werkgeversportaal van het UWV is en door het UWV ter beschikking wordt gesteld aan werkgevers. Ook blijkt dat het UWV de doeleinden bepaalt van de gegevensverwerkingen die in het portaal plaatsvinden. Het UWV bepaald derhalve het doel en de middelen van de

[33] Zie voor een uitgebreid overzicht hoofdstuk 4, paragraaf 2 van dit rapport.

gegevensverwerking. Daarmee is UWV verantwoordelijke als bedoeld in artikel 1, onder d, Wbp voor deze gegevensverwerkingen.

5.3 Bijzondere persoonsgegevens

Gegevens over de gezondheid

Zoals aangegeven in het juridisch kader vallen onder het begrip gezondheidsgegevens in de zin van artikel 16 Wbp niet alleen gegevens waarop het medisch beroepsgeheim rust (zoals de aard, oorzaak en de behandeling van de ziekte) maar alle gegevens die de geestelijke of lichamelijke gezondheid van een persoon treffen, waaronder het enkele gegeven dat iemand ziek is.

In het werkgeversportaal van het UWV worden onder meer de volgende persoonsgegevens verwerkt:

- Brieven aan werkgevers waaronder beschikkingen in pdf
- Meetellen voor quotumregeling en/of banenafspraak
- Datum eerste AO-dag
- Datum laatste AO-dag
- Percentage loondoorbetaling tijdens AO
- Zieke uitzendkracht
- Zieke oproepkracht
- Ziek uit dienst
- Ziek tgv zwangerschap
- Ziek tgv bevalling
- Ziek tgv orgaandonatie
- Samenloop met WIA
- Samenloop met WAO of WAZ of 5 jaar voorafgaand
- Jonger dan 18 jaar en onderwijs belemmering
- Recht op WAJONG-uitkering voorafgaande dienstbetrekking
- Ontvangst WAJONG-uitkering of ooit gehad
- Oordeel CWI functionele beperking
- Indicatiestelling WSW
- Arbeidsovereenkomst op grond van artikel 7 WSW
- Recht op voorziening t.b.v. arbeidsgeschiktheid
- Zwangerschapsverlof
- Verlengd bevallingsverlof
- Arbeidsongeschiktten gevolge van zwangerschap
- Overlijden

Deze gegevens hebben, op zichzelf staand en/of in samenhang met elkaar, betrekking op de lichamelijke en/of geestelijke gezondheid van personen en zijn daarmee gegevens over gezondheid zoals bedoeld in artikel 16 Wbp.

Een verwerking van gezondheidsgegevens is altijd aan een geheimhoudingsplicht onderworpen. Deze geheimhoudingsplicht vloeit voort uit ambt, beroep, wettelijk voorschrift of een overeenkomst tot geheimhouding, dan wel uit artikel 21, tweede lid, tweede volzin, Wbp, waarin het volgende is aangegeven: "*In de gevallen als bedoeld in het eerste lid worden de gegevens alleen verwerkt door personen die uit hoofde van ambt, beroep of wettelijk voorschrift, dan wel krachtens een overeenkomst tot geheimhouding zijn verplicht. Indien de verantwoordelijke gegevens persoonlijk verwerkt en op hem niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift een geheimhoudingsplicht rust, is hij verplicht tot geheimhouding van de gegevens, behoudens voor zover de wet hem tot*

mededeling verplicht of uit zijn taak de noodzaak voortvloeit dat de gegevens worden meegedeeld aan anderen die krachtens het eerste lid bevoegd zijn tot verwerking daarvan.".

In de zienswijze van 21 juni 2017 stelt UWV: "*Tot slot zijn in onze ogen de gezondheidsgegevens, die iemand zou kunnen inzien na onbevoegd inloggen op het portaal, gelimiteerd tot een beperkte set van gezondheidsgegevens die niet verwerkt hoeven te worden onder Wet BIG.*"
Het UWV heeft in de bijlage bij de zienswijze de volgende gegevens gemarkeerd als gegevens over de gezondheid:

- Brieven aan werkgevers, waaronder beschikkingen
- Meetellen voor quotumregeling en/of banenafspraak
- Datum eerste AO-dag
- Datum laatste AO-dag
- Percentage loondoorbetaling tijdens AO
- Datum bevalling
- Datum gewenste ingang zwangerschapsverlof
- Datum vermoedelijke bevalling

De AP merkt op dat het voor de vaststelling van het feit of een persoonsgegeven een gegeven over de gezondheid betreft niet relevant is of de gegevens over de gezondheid al dan niet verwerkt worden onder de Wet BIG.[34] Zoals in het juridisch kader is weergegeven vallen onder het begrip gezondheidsgegevens in de zin van artikel 16 Wbp niet alleen gegevens waarop het medisch beroepsgeheim rust (zoals de aard, oorzaak en de behandeling van de ziekte) maar álle gegevens die de geestelijke of lichamelijke gezondheid van een persoon treffen. Tevens merkt de AP op dat gegevens over de gezondheid altijd zijn onderworpen aan tenminste de geheimhoudingsplicht van artikel 21, tweede lid, tweede volzin, Wbp.

Ten aanzien van de overige gegevens die de AP noemt in de opsomming aan het begin van deze paragraaf stelt het UWV in de bijlage bij de zienswijze dat dit gegevens zijn "*die niet worden getoond, want gecodeerd en alleen code is zichtbaar.*" UWV geeft hierbij een overzicht van 36 gegevens die niet in het portaal zichtbaar zouden zijn, waaronder gegevens over de gezondheid zoals zwangerschapsverlof, ongeval, ziek ten gevolge van bevalling, recht op Wajonguitkering en arbeidsongeschiktheid ten gevolge van zwangerschap.

Inmiddels is vastgesteld dat de gegevens niet gecodeerd in het systeem staan en dus wel zichtbaar zijn. Naar aanleiding van de zienswijze heeft de AP het UWV namelijk nadere vragen gesteld over deze coderingen[35] en heeft de AP, op uitnodiging van het UWV, ten kantore van het UWV in het werkgeversportaal gekeken. Hieruit bleek dat er geen sprake is van het werken met coderingen, de gegevens worden ongecodeerd aan de werkgevers getoond.
Bij brief van 25 juli stelt het UWV: "*Uw inspecteurs hebben op 18 juli jl. een bezoek aan UWV gebracht. Tijdens dit bezoek is vastgesteld dat de gegevens die in de bijlage bij onze zienswijze zijn opgenomen niet als code maar als tekst worden getoond op het Werkgeversportaal. De zinsnede dat daarbij alleen de codes zichtbaar zijn voor werkgevers, blijkt daarmee gebaseerd op een onjuiste veronderstelling van UWV zelf. De codes worden slechts verwerkt op de technische koppelvlakken voor intern gebruik.[…].*"

[34] De AP gaat ervan uit dat het UWV hiermee doelt op het feit dat het medisch beroepsgeheim niet van toepassing is op een beperkte set van gegevens die de bedrijfsarts in het kader van de begeleiding en/of re-integratie van zieke werknemers aan de werkgever mag verstrekken.
[35] Brief van 11 juli 2017 van de AP aan het UWV.

Tevens stelt het UWV in de zienswijze van 21 juni 2017: "*Het werkgeversportaal maakt een onderscheid tussen informatie die via het werkgeversportaal van werkgever aan UWV gestuurd wordt (postbusfunctie) en informatie die door werkgevers wordt gedeeld en voor werkgevers toegankelijk blijft (portaalfunctie) […].*
Uit de zienswijze van het UWV en het onderzoek dat de AP bij het UWV heeft uitgevoerd blijkt dat het re-integratieverslag dat door een werkgever digitaal ingestuurd kan worden naar het UWV via de postbusfunctie van het werkgeversportaal, niet ingezien kan worden door iemand die onbevoegd toegang krijgt tot het portaal. Het re-integratieverslag is dan ook door de AP verwijderd uit de in de voorlopige bevindingen genoemde opsomming van gegevens over de gezondheid van werknemers die in het werkgeversportaal worden verwerkt.

Uit bovenstaande volgt dat er gegevens over de gezondheid worden verwerkt in het werkgeversportaal van het UWV. Dit betreffen tenminste de gegevens die aan het begin van deze paragraaf worden opgesomd.

5.4 Beveiliging van het werkgeversportaal

Ingevolge artikel 13 van de Wbp dient een verantwoordelijke passende technische en organisatorische maatregelen ten uitvoer te brengen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Deze maatregelen moeten, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau garanderen gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen.

Norm
Uit het juridisch kader (zie hoofdstuk 3) blijkt dat een verantwoordelijke bij de ontsluiting van een verwerking van gegevens over de gezondheid via internet aan de in artikel 13 Wbp bepaalde norm 'passende maatregelen' uitvoering dient te geven.

Voor de beveiliging van bijzondere persoonsgegevens waarop het medisch beroepsgeheim en/of een bijzondere, wettelijk bepaalde geheimhoudingsplicht rust, het betrouwbaarheidsniveau 'hoog' van toepassing.[36,37] Dit betekent dat in ieder geval sprake moet zijn van meerfactorauthenticatie bij het verkrijgen van toegang tot het systeem via internet.
Zoals in de vorige paragraaf is beschreven verwerkt het UWV In het werkgeversportaal een veelvoud aan gegevens over de gezondheid van (veelal zieke) werknemers. Op de verwerkte gegevens rust het medisch beroepsgeheim en/of een bijzondere, wettelijk bepaalde geheimhoudingsplicht, namelijk in ieder geval de geheimhoudingsplicht zoals deze is bepaald in artikel 21, tweede lid, tweede volzin, Wbp. Het UWV verschaft toegang tot het werkgeversportaal via internet. Het UWV dient derhalve in ieder geval gebruik te maken van meerfactorauthenticatie als passende maatregel (artikel 13 Wbp) om de risico's op onrechtmatige verwerking te beheersen bij het verlenen van toegang tot het werkgeversportaal via internet.

Werkwijze UWV
Op de website van het UWV is beschreven hoe de autorisatie tot het werkgeversportaal plaatsvindt:
"*Als u een account wilt aanvragen, ga dan naar uwv.nl/werkgeversportaal en klik op 'Een account aanvragen'. Uw account is gekoppeld aan uw e-mailadres. U kunt zelf een wachtwoord kiezen. U krijgt ter bevestiging van uw aanvraag een e-mail*

[36] Betrouwbaarheidsniveaus voor digitale dienstverlening, een handreiking voor overheidsorganisatie, Forum Standaardisatie, november 2016, pag. 33.
[37] Betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten, een handreiking voor overheidsorganisaties, Forum Standaardisatie, augustus 2014, pag. 22 en pag. 27.

van UWV. Klik op de link in deze e-mail om uw accountaanvraag af te ronden. Met uw e-mailadres en wachtwoord kunt u voortaan inloggen."
Werkgevers krijgen toegang tot de persoonsgegevens in het werkgeversportaal door het invoeren van een gebruikersnaam (het e-mailadres) ter identificatie van de gebruiker en een wachtwoord ter authenticatie. Er is derhalve sprake van authenticatie met één factor (het wachtwoord).

Het UWV stelt in de correspondentie met de AP: [38] "*Ook wij hebben geconstateerd dat ons werkgeversportaal nog niet voldoet aan de beveiligingseisen die voortvloeien uit artikel 13 Wbp. De toegang tot het werkgeversportaal wordt inderdaad nog niet middels tweefactor-authenticatie verkregen. Dat is echter wel gewenst."*

Het UWV past op dit moment geen meerfactorauthenticatie toe bij het verlenen van toegang tot het werkgeversportaal via internet.

Passende maatregelen
Het UWV heeft in de brief van 25 januari 2016 aangegeven gebruik te willen gaan maken van eHerkenning, maar dat dat op dit moment nog niet mogelijk is. Het UWV stelt in de brief: "*de beveiligingsrisico's worden door UWV nu nog beperkt door het doen van penetratie- en securitytesten."*
In de brief van 3 augustus 2016 stelt het UWV: "*UWV voert bovendien jaarlijks penetratie- en securitytesten uit. Op basis van deze analyses vindt bijsturing plaats op de huidige beveiligingsmaatregelen."*
In dezelfde brief geeft het UWV tevens een overzicht van de beveiligingsmaatregelen die het UWV heeft getroffen voor de beveiliging van het werkgeversportaal, zoals onder andere het uitvoeren van, continu login van en monitoring op het gebruik en, indien zich signalen voordoen, onderzoek hiernaar, bewaking met een Web Applicatie Firewall, een Intrusion Prevention Systeem en Anti-(D)DOS dienst.[39]

Het uitvoeren van jaarlijkse penetratie- en securitytesten[40] en de overige door het UWV getroffen beveiligingsmaatregelen zien echter niet op een veiliger toegang van gebruikers tot de applicaties (authenticatie). Deze maatregelen die het UWV heeft getroffen zijn derhalve ten aanzien van de authenticatie niet passend en kunnen ook niet passend zijn, nu deze geen passend beschermingsniveau bieden voor het verkrijgen van toegang tot de applicatie.

In de zienswijze van 21 juni 2017 stelt het UWV: *"Wij hebben naar aanleiding van uw brieven in december 2016 en januari 2017 onderzoek gedaan naar tijdelijke mogelijkheden meerfactor authenticatie voor het werkgeversportaal. Uit dat onderzoek bleek dat een tijdelijke voorziening – ten opzichte van de implementatie van eHerkenning – een beperkte tijdwinst oplevert. Het is in onze ogen niet doelmatig en proportioneel om gelijktijdig twee implementatietrajecten te doorlopen die tweefactorauthenticatie bewerkstelligen. Dit leidt tot extra administratieve lasten voor werkgevers en ondoelmatige inzet van publieke middelen. Vandaar dat UWV in april 2017 heeft besloten de implementatie van de eHerkenning op te starten. Dit is mede mogelijk, omdat het technische knelpunt voor UWV rond de implementatie van eHerkenning – het identificeren van organisaties via het RSIN – sinds 1 juni jongstleden is weggenomen. Hiermee bewerkstelligen we onze ambitie om het beveiligingsniveau op onze portalen te verhogen naar niveau 'substantieel' waarmee we aan de door de Autoriteit Persoonsgegevens (AP) gestelde norm zullen voldoen. […] Momenteel werkt UWV aan de eerste fase van de implementatie: het vooronderzoek. We verwachten in mei de aansluiting op eHerkenning*

[38] Brief van 25 januari 2016 van het UWV aan de AP.
[39] Zie paragraaf 4.3 voor een uitgebreide opsomming van deze beveiligingsmaatregelen van het UWV.
[40] Ten overvloede merkt de AP op dat het passend is, om zeker in het geval van een applicatie waarin medische gegevens worden verwerkt, meerdere penetratietesten/scans per jaar uit te voeren omdat er doorlopend nieuwe risico's kunnen ontstaan, onder andere doordat er doorlopend nieuwe beveiligingslekken in de gebruikte software kunnen ontstaan. Zie hiervoor ook het onderzoek van de AP naar *'de beveiliging van Humannet Starter en Humannet Verzuim door VCD Humannet B.V.'*, z2012-00288, december 2014.

gerealiseerd te hebben. Wij stellen voor in oktober 2017 te rapporteren over de voortgang van de implementatie van eHerkenning, eventueel in bestuurlijk overleg. Het vooronderzoek is dan afgerond. Wij zetten hiermee alle zeilen bij om eHerkenning zo snel mogelijk geïmplementeerd te hebben."

UWV stelt voorts in de zienswijze: "gedurende de implementatie van eHerkenning willen we graag dat werkgevers gebruik kunnen blijven maken van onze portalen. De Wet bescherming persoonsgegevens (Wbp) verplicht UWV om een passend beveiligingsniveau te borgen gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen. We hechten daar zelf ook grote waarde aan. Wij achten het verantwoord om binnen het huidige beveiligingsbeleid te koersen op realisatie van tweefactorauthenticatie via de structurele overheidsbrede oplossing eHerkenning. Dit omdat wij het risico op inbreuk op de gezondheidsgegevens in ons werkgeversportaal laag achten, mede door de beveiligingsmaatregelen als geautomatiseerde monitoring op logging en penetratie- en securitytesten zoals ook verwoord in de voorlopige bevindingen op pagina 19. Dit wordt bevestigd in het uitgevoerde BIRA onderzoek door Noordbeek IT Audit, Compliance & Advisory. Wij blijven in onze verbetercycli streven naar verhoging van de beveiliging op ons portaal. Er zijn ons op dit moment vanuit onze eigen beveiligingsteams of vanuit externe bronnen geen signalen bekend van misbruik van de genoemde gezondheidsgegevens.

In het BIRA[41] rapport, dat de AP naar aanleiding van bovenstaande heeft opgevraagd bij het UWV, staat in de conclusie waar het UWV naar verwijst: "*Het risico van misbruik van de persoonsgegevens in het Werkgeversportaal door derden, anders dan door personeel van de werkgever of intermediair zelf, is laag*."
In hetzelfde BIRA rapport staat echter ook het volgende:[42] "*Identity and Access Management (IAM) van het Werkgeversportaal voldoet aan de in redelijkheid daaraan te stellen eisen vanuit IB&P (afgezien van de deficiëntie 'two factor authentication')*.

In de brief van 26 juli 2017 van het UWV somt het UWV enkele maatregelen op die zij heeft getroffen ten aanzien van het beheer van accounts, zoals aanpassing van de gebruikersvoorwaarden en de invoering van een operationeel Secure Software Development (SSD) proces. Ook noemt het UWV enkele voorgenomen aanpassingen ten aanzien van de invoering van de AVG en de implementatie van eHerkenning.

Zoals gesteld in het juridisch kader moet voor de beveiliging van gegevens waarop het medisch beroepsgeheim en/of een bijzondere, wettelijk bepaalde geheimhoudingsplicht rust, in ieder geval sprake zijn van meerfactorauthenticatie bij het verkrijgen van toegang tot het systeem via internet.
Het feit dat het UWV zelf dan wel een externe partij van mening is dat het risico op inbreuk op de gezondheidsgegevens in het werkgeversportaal laag is, maakt niet dat de norm ten aanzien van de verwerking van gegevens over de gezondheid in een dergelijk systeem niet meer van toepassing is. De aard van deze gegevens en het feit dat toegang tot het systeem via internet verloopt maakt dat deze norm van toepassing is.
Alleen als het UWV maatregelen heeft getroffen die zorgdragen voor een veiliger toegang van gebruikers tot de applicatie, zoals meerfactorauthenticatie, voldoet UWV aan het bepaalde in artikel 13 Wbp.

Het UWV heeft er voor gekozen om voor de verwerking van de gegevens over de gezondheid van werknemers een applicatie aan te bieden die via internet wordt ontsloten. Met deze werkwijze als uitgangspunt geldt dat meerfactorauthenticatie vereist is.

Concluderend

[41] Rapport van Bevindingen Business IB&P Requirements Analyse op K&S Werkgeversportaal, versie 1.0, 23 februari 2017, pag. 8.
[42] Rapport van Bevindingen Business IB&P Requirements Analyse op K&S Werkgeversportaal, versie 1.0, 23 februari 2017, pag. 7.

Uit artikel 13 Wbp vloeit voort dat een verantwoordelijke passende maatregelen moet treffen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Gegeven de gevoeligheid van de persoonsgegevens die in het werkgeversportaal van het UWV worden verwerkt, namelijk gegevens over de gezondheid van (veelal zieke) werknemers, dient het verkrijgen van toegang tot dit systeem via internet, gelet op de huidige stand van de techniek, plaats te vinden middels meerfactorauthenticatie. De Autoriteit Persoonsgegevens heeft het UWV vanaf 25 november 2015 gewezen op het feit dat voor het inloggen op het werkgeversportaal door alle gebruikers gebruik dient te worden gemaakt van meerfactorauthenticatie.
Het UWV heeft in de zienswijze van 21 juni 2017 aangegeven dat zij momenteel werkt aan de eerste fase van de implementatie, te weten het vooronderzoek naar eHerkenning. Het UWV verwacht in mei 2018 de aansluiting op eHerkenning gerealiseerd te hebben. Tot die tijd zal het portaal toegankelijk voor gebruikers zijn zonder gebruik van meerfactorauthenticatie.
De door het UWV aangedragen maatregelen om de risico's te beheersen gedurende de periode dat eHerkenning nog niet in gebruik genomen is - zoals het uitvoeren van jaarlijkse penetratie- en securitytesten - zien niet op een veiliger toegang van gebruikers tot de applicaties (authenticatie). Deze maatregelen die het UWV heeft getroffen zijn derhalve niet passend.

Het UWV past op dit moment geen meerfactorauthenticatie toe bij het verlenen van toegang tot het werkgeversportaal noch heeft het UWV er op een andere manier zorg voor gedragen dat passende maatregelen zijn getroffen ten aanzien van het verkrijgen van toegang tot de gegevens in het werkgeversportaal. Er is hierdoor sprake van een voortdurende overtreding die geen incidenteel maar structureel karakter heeft, nu deze overtreding veel mensen raakt en al een langere periode voortduurt. Het UWV handelt daarmee in strijd met artikel 13 Wbp.

6. Conclusie

Het UWV verwerkt gegevens over de gezondheid van werknemers in het werkgeversportaal. Werkgevers krijgen via internet toegang tot de persoonsgegevens in het portaal door het invoeren van een gebruikersnaam en een wachtwoord.

Uit artikel 13 Wbp vloeit voort dat een verantwoordelijke passende maatregelen moet treffen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Gegeven de gevoeligheid van de persoonsgegevens die in het werkgeversportaal van het UWV worden verwerkt, namelijk gegevens over de gezondheid van (veelal zieke) werknemers, dient het verkrijgen van toegang tot dit systeem via internet, gelet op de huidige stand van de techniek, plaats te vinden middels meerfactorauthenticatie. De Autoriteit Persoonsgegevens heeft het UWV vanaf 25 november 2015 gewezen op het feit dat voor het inloggen op het werkgeversportaal door alle gebruikers gebruik dient te worden gemaakt van meerfactorauthenticatie.
Het UWV heeft in de zienswijze van 21 juni 2017 aangegeven dat zij momenteel werkt aan de de eerste fase van de implementatie, te weten het vooronderzoek naar eHerkenning. Het UWV verwacht in mei 2018 de aansluiting op eHerkenning gerealiseerd te hebben. Tot die tijd zal het portaal toegankelijk voor gebruikers zijn zonder gebruik van meerfactorauthenticatie.
De door het UWV aangedragen maatregelen om de risico's te beheersen gedurende de periode dat eHerkenning nog niet in gebruik genomen is - zoals het uitvoeren van jaarlijkse penetratie- en securitytesten - zien niet op een veiliger toegang van gebruikers tot de applicaties (authenticatie). Deze maatregelen die het UWV heeft getroffen zijn derhalve niet passend.

Het UWV past op dit moment geen meerfactorauthenticatie toe bij het verlenen van toegang tot het werkgeversportaal noch heeft het UWV er op een andere manier zorg voor gedragen dat passende maatregelen zijn getroffen ten aanzien van het verkrijgen van toegang tot de gegevens in het werkgeversportaal. Er is hierdoor sprake van een voortdurende overtreding die geen incidenteel maar structureel karakter heeft, nu deze overtreding veel mensen raakt en al een langere periode voortduurt. Het UWV handelt daarmee in strijd met artikel 13 Wbp.

AUTORITEIT
PERSOONSGEGEVENS

Contactgegevens

Bezoekadres
(alleen volgens afspraak)
Bezuidenhoutseweg 30
2594 AV DEN HAAG

Let op: bij bezoek aan de Autoriteit Persoonsgegevens moet u een geldig identiteitsbewijs laten zien.

Postadres
Postbus 93374
2509 AJ DEN HAAG

Telefonisch spreekuur
Op onze website autoriteitpersoonsgegevens.nl vindt u informatie en antwoorden op vragen over de bescherming van persoonsgegevens. Heeft u op deze website geen antwoord op uw vraag gevonden? Dan kunt u contact opnemen met de publieksvoorlichters van de Autoriteit Persoonsgegevens tijdens het telefonisch spreekuur via telefoonnummer **0900-2001201**. De publieksvoorlichters zijn bereikbaar op maandag, dinsdag, donderdag en vrijdag van 10.00 tot 12.00 uur. (5 cent per minuut, plus de kosten voor het gebruik van uw mobiele of vaste telefoon).

Persvoorlichting
Journalisten en redacteuren kunnen met vragen terecht bij de woordvoerders van de Autoriteit Persoonsgegevens via telefoonnummer **070-8888555**.

Zakelijke relaties
Bent u een zakelijke relatie van de Autoriteit Persoonsgegevens, zoals een leverancier, dan kunt u ons telefonisch bereiken via telefoonnummer **070-8888500**.

Over de Autoriteit Persoonsgegevens
Iedereen heeft recht op een zorgvuldige omgang met zijn persoonsgegevens. De Autoriteit Persoonsgegevens houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens en adviseert over nieuwe regelgeving.