AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Bezuidenhoutseweg 30, 2594 AV Den Haag
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

Aangetekend
UWV
Raad van Bestuur
Postbus 58285
1040 HG Amsterdam

Datum
31 juli 2018

Ons kenmerk
z2018-02009

Contactpersoon
[VERTROUWELIJK]
070 8888 500

Onderwerp
Last onder dwangsom

Samenvatting

1. De Autoriteit Persoonsgegevens (hierna: de AP) heeft op 27 maart 2017 op grond van artikel 60 van de Wet bescherming persoonsgegevens (hierna: de Wbp), zoals dat destijds gold, een onderzoek ingesteld naar het gebruik van meerfactorauthenticatie in het werkgeversportaal van het Uitvoeringsinstituut Werkgeversverzekeringen (hierna: het UWV).

2. Het UWV verwerkt in het werkgeversportaal onder meer persoonsgegevens die betrekking hebben op de gezondheid van werknemers. Gelet hierop dient toegang tot het werkgeversportaal via internet plaats te vinden middels meerfactorauthenticatie. Het UWV past op dit moment éénfactorauthenticatie toe bij het verlenen van toegang tot het werkgeversportaal.

3. De AP heeft in het rapport definitieve bevindingen (hierna: het onderzoeksrapport) geconstateerd dat het UWV daarmee in strijd handelt met artikel 13 van de Wbp, zoals dat destijds gold, op grond waarvan, voor zover hier van belang, een verantwoordelijke passende maatregelen moet treffen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.

4. De AP baseert het dwangsombesluit op het onderzoeksrapport, de door het UWV mondeling gegeven zienswijze op het voornemen van de AP om een last onder dwangsom op te leggen en de nadien door het UWV op verzoek van de AP verstrekte informatie

5. Op 25 mei 2018 is de Algemene verordening gegevensbescherming (hierna: de AVG) van toepassing geworden. De AVG stelt in artikel 32, eerste lid, dezelfde verplichting, zoals die gold op grond van artikel 13

van de Wbp. Nu deze overtreding nog immer voortduurt, overtreedt het UWV artikel 32, eerste lid, van de AVG.

6. Het UWV wenst aan te sluiten op het stelsel van eHerkenning om op deze wijze meerfactorauthenticatie bij het verlenen van toegang tot het werkgeversportaal te kunnen realiseren. De datum waarop UWV verwacht dat alleen nog door gebruik van eHerkenning kan worden ingelogd op het werkgeversportaal is sinds de eerste uitvraag door de AP bij brief van 25 november 2015 inmiddels opgeschoven naar 1 november 2019.

7. Naar aanleiding van het bovenstaande heeft de AP besloten om op grond van artikel 16, eerste lid, van de Uitvoeringswet Algemene verordening gegevensbescherming (hierna: UAVG) in samenhang bezien met artikel 5:32, eerste lid, van de Algemene wet bestuursrecht (hierna: de Awb) een last onder dwangsom op te leggen. Met de last onder dwangsom beoogt de AP te verzekeren dat aan de geconstateerde overtreding een einde wordt gemaakt.

8. Uiterlijk op 31 oktober 2019 moet het verlenen van toegang tot het werkgeversportaal van een passend beveiligingsniveau zijn voorzien, waarbij inloggen in het portaal alleen mogelijk is door middel van een passende vorm van meerfactorauthenticatie. Onderdeel van die last is dat het UWV het vereiste betrouwbaarheidsniveau opnieuw dient te bepalen door een risicoanalyse uit te voeren aan de hand van de meest recente versie van de Handreiking 'Betrouwbaarheidsniveaus voor digitale dienstverlening, een handreiking voor overheidsorganisaties' (versie 4).

9. Bij het niet naleven van de last na het verstrijken van de begunstigingstermijn is UWV een dwangsom van EUR 150.000 verschuldigd voor iedere maand dat de last niet (geheel) is uitgevoerd, met een maximum van EUR 900.0000.

Verloop van de procedure

10. Op 29 augustus 2017 heeft de AP het onderzoeksrapport vastgesteld en aan het UWV verzonden. De openbare versie van het rapport is op 14 november 2017 gepubliceerd op de website van de AP.

11. Bij brief van 15 augustus 2017 heeft de AP naar aanleiding van het onderzoek aan het UWV nog enkele vragen gesteld over de omvang van het werkgeversportaal.

12. Bij brief van 30 augustus 2017 heeft het UWV gereageerd op de vragen die de AP bij brief van 15 augustus 2017 heeft gesteld.

13. Bij brief van 11 september 2017 heeft het UWV haar reactie gegeven op het onderzoeksrapport. Het UWV geeft hierin onder meer aan te onderkennen dat het beveiligingsniveau niet voldoet aan de eisen van artikel 13 van de Wbp en dit te willen verhelpen door de implementatie van eHerkenning niveau substantieel.

14. Bij brief van 9 november 2017 heeft het UWV de AP geïnformeerd over de voortgang van de implementatie van eHerkenning.

15. De AP heeft het UWV bij brief van 14 december 2017 in kennis gesteld van haar voornemen om een last onder dwangsom op te leggen en het UWV in de gelegenheid gesteld mondeling of schriftelijk haar zienswijze naar voren te brengen. Het UWV is daarbij uitgenodigd voor een hoorzitting.

16. Op 6 februari 2018 heeft de hoorzitting plaatsgevonden. Van de hoorzitting is een verslag gemaakt, dat als **bijlage 1** bij dit besluit is gevoegd.

17. Naar aanleiding van hetgeen tijdens de hoorzitting is besproken, heeft het UWV bij brief van 28 februari 2018 aanvullende informatie gegeven en nadere documenten verstrekt, waaronder het projectplan eHerkenning.

18. Naar aanleiding van de bij brief van 28 februari 2018 ontvangen informatie heeft de AP aan het UWV bij brief van 15 maart 2018 vragen gesteld.

19. Bij brief van 3 april 2018 heeft het UWV gereageerd op de vragen van de AP van 15 maart 2018 en hierbij de 'risicoanalyse verzuimmelder' (hierna: de risicoanalyse) verstrekt.

20. Naar aanleiding van de bij brief van 3 april 2018 ontvangen informatie heeft de AP aan het UWV bij brief van 14 mei 2018 vragen gesteld.

21. Bij brief van 25 mei 2018 heeft het UWV gereageerd op de vragen van de AP van 14 mei 2018.

Onderzoeksrapport

22. In het onderzoeksrapport heeft de AP geconstateerd dat het UWV in het werkgeversportaal persoonsgegevens over gezondheid verwerkt. Toegang tot het werkgeversportaal wordt verkregen door het invoeren van een e-mailadres en wachtwoord. Dit is een vorm van éénfactorauthenticatie.

23. Uit artikel 13 van de Wbp - thans artikel 32, eerste lid, van de AVG - vloeit voort dat een verantwoordelijke passende maatregelen moet treffen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Het begrip 'passend' duidt mede op een proportionaliteit tussen beveiligingsmaatregelen en de aard van de te beschermen gegevens. Gegeven de gevoeligheid van de persoonsgegevens die in het werkgeversportaal van het UWV worden verwerkt, namelijk gegevens over de gezondheid van werknemers, dient het verkrijgen van toegang tot het portaal via internet, gezien de stand van de techniek, plaats te vinden middels ten minste meerfactorauthenticatie.

24. Het UWV heeft aangegeven maatregelen genomen te hebben om toegang door onbevoegden tot het werkgeversportaal te voorkomen, zoals het jaarlijks uitvoeren van penetratie- en securitytesten en het continu loggen van en monitoren op het gebruik. Deze maatregelen zijn ten aanzien van de authenticatie niet passend omdat ze geen passend beschermingsniveau kunnen bieden voor het verkrijgen van toegang

tot de applicatie. Doordat het UWV geen meerfactorauthenticatie toepast, noch op een andere manier passende maatregelen heeft getroffen ten aanzien van het verkrijgen van toegang tot de gegevens in het werkgeversportaal, handelt het UWV in strijd met artikel 13 van de Wbp, zoals dat destijds gold.

Wettelijk kader

25. Het relevante wettelijk kader is opgenomen als **bijlage 2** bij dit besluit.

AVG

26. In het onderzoeksrapport heeft de AP een overtreding van de norm uit artikel 13 van de Wbp geconstateerd. Per 25 mei 2018 zijn de AVG en UAVG van toepassing en is de Wbp ingetrokken.

27. Bij de beoordeling of ook sprake is van een overtreding van de norm uit de AVG, is van belang dat de norm onder de AVG materieel niet wezenlijk wijzigt ten opzichte van de norm onder de Wbp.
De norm uit artikel 13 van de Wbp is thans neergelegd in artikel 32, eerste en tweede lid, van de AVG. Laatstgenoemd artikel stelt dat de verwerkingsverantwoordelijke, rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, passende technische en organisatorische maatregelen moet nemen om een op het risico afgestemd beveiligingsniveau te waarborgen. Deze verplichting komt materieel overeen met de verplichting uit artikel 13 van de Wbp.

28. Dit betekent dat, aangezien de onderzochte feiten en de relevante omstandigheden na de totstandkoming van het onderzoeksrapport tot op heden niet gewijzigd zijn, met ingang van 25 mei 2018 sprake is van overtreding van artikel 32, eerste lid, van de AVG.

Zienswijze

29. Naar aanleiding van het voornemen van de AP om een last onder dwangsom op te leggen heeft het UWV tijdens de hoorzitting van 6 februari 2018 mondeling een zienswijze gegeven. Samengevat komt die zienswijze er op neer dat het UWV erkent dat de beveiliging van het werkgeversportaal niet voldoet aan de eisen die voortvloeien uit artikel 13 van de Wbp en thans artikel 32, eerste lid, van de AVG omdat het UWV geen meerfactorauthenticatie toepast op het verlenen van toegang tot het portaal.

30. Het UWV heeft in april 2017 besloten te starten met de implementatie van eHerkenning niveau 3/substantieel, waarbij meerfactorauthenticatie wordt toegepast en zodoende de overtreding van artikel 13 van de Wbp en thans artikel 32, eerste, van de AVG wordt opgeheven. Het UWV heeft bij het bepalen van het betrouwbaarheidsniveau het feit dat in het werkgeversportaal alleen gezondheidsgegevens worden verwerkt die zien op het ziekmelden of het feit dat iemand zwanger is.
De aard van de ziekmelding wordt niet verwerkt.

31. Het UWV heeft naar voren gebracht andere oplossingen te hebben onderzocht maar de aansluiting op eHerkenning als enige reële mogelijkheid te zien om meerfactorauthenticatie te bewerkstelligen. Met de komst van de Wet digitale overheid (hierna: Wdo) is het namelijk de bedoeling dat alle overheidspartijen gebruik maken van de middelen die in deze wet zijn opgenomen.

32. Bij de implementatie van eHerkenning is het UWV deels afhankelijk van derden en loopt het UWV tegen een aantal problemen aan, waardoor de implementatie langer op zich laat wachten dan het UWV had gehoopt.

Beoordeling

Beoordelingskader

33. In het onderzoeksrapport heeft de AP vastgesteld dat het UWV in het werkgeversportaal persoonsgegevens, waaronder bijzondere persoonsgegevens, verwerkt. Het betreft onder andere NAW-gegevens, BSN, financiële gegevens en gegevens over arbeidsongeschiktheid, ontslag en bevalling. Werkgevers kunnen via internet op het portaal inloggen door een e-mailadres en wachtwoord in te voeren. Dit is een vorm van éénfactorauthenticatie [1]. Uit de stukken en het verhandelde ter hoorzitting is gebleken dat deze situatie thans niet is gewijzigd.

34. Artikel 32, eerste lid, van de AVG bepaalt dat de verantwoordelijke passende technische en organisatorische maatregelen moet nemen om persoonsgegevens te beveiligen tegen verlies of onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen.

35. Dit betekent dat de verantwoordelijke, in dit geval het UWV, een vertaalslag moet maken van de risico's voor de betrokkene wiens persoonsgegevens worden verwerkt naar de betrouwbaarheidseisen waaraan de dienst die wordt aangeboden (het werkgeversportaal) moet voldoen en die binnen het vakgebied informatiebeveiliging als de meest recente en representatieve invulling daarvan wordt gezien.

36. Bij het bepalen van het risico voor de betrokkene zijn onder andere de aard van de persoonsgegevens en de aard van de verwerking van belang: deze factoren bepalen de potentiële schade voor de individuele betrokkene bij bijvoorbeeld verlies, wijziging of onrechtmatige verwerking van de gegevens. Bij het maken van de vertaalslag naar het betrouwbaarheidsniveau van het werkgeversportaal kan het UWV gebruik maken van de Handreiking 'Betrouwbaarheidsniveaus voor digitale dienstverlening, een handreiking voor overheidsorganisaties, versie 4' van Forum Standaardisatie (hierna: de Handreiking).

37. Het gebruik van deze Handreiking is weliswaar niet verplicht, maar biedt een beoordelingskader voor overheidsorganisaties voor het bepalen van betrouwbaarheidsniveaus voor digitale dienstverlening

[1] Authenticatie is het proces waarbij wordt nagegaan of een gebruiker die in wil loggen in een applicatie/systeem daadwerkelijk is wie hij/zij beweert te zijn.

waarvan kan worden aangenomen dat het in zoverre de meest recente inzichten en eisen weerspiegelt. Beveiligingsstandaarden geven vervolgens, na het vaststellen van het van toepassing zijnde betrouwbaarheidsniveau, houvast bij het treffen van passende maatregelen.[2]

38. De AP heeft onderzocht of het UWV passende maatregelen heeft getroffen ten aanzien van authenticatie bij het inloggen op het werkgeversportaal. De AP heeft zich in haar onderzoek enkel gericht op de aard van de te beschermen persoonsgegevens, hetgeen zich vertaalt naar een minimaal te hanteren beveiligingsniveau. De beoordeling in dit besluit is dan ook uitsluitend gebaseerd op de aard van de te beschermen persoonsgegevens. Niet is uitgesloten dat andere factoren dan de aard van de persoonsgegevens een hoger beveiligingsniveau vereisen. De AP kan evenwel niet, zoals hierna nog aan de orde zal komen, voor of in de plaats van het UWV alle – in Handreiking versie 4 opgenomen - relevante factoren beoordelen. Het is aan het UWV om deze factoren te betrekken in een risicoanalyse om zodoende het juiste beveiligingsniveau te bepalen.[3]

Gegevens betreffende iemands gezondheid

39. In artikel 4, onderdeel 15, van de AVG wordt de volgende definitie gegeven: 'gegevens over de gezondheid zijn persoonsgegevens die verband houden met de fysieke of mentale toestand van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven'. Onder de AVG blijft onveranderd dat het begrip 'gezondheidsgegevens' ruim moet worden opgevat: het omvat niet alleen de gegevens die een arts bij een medisch onderzoek of medische behandeling verwerkt, maar álle gegevens die de geestelijke of lichamelijke gezondheid van een persoon treffen. Zo is het enkele gegeven dat iemand zich ziek heeft gemeld een gegeven over de gezondheid, ook al zegt dat niets over de aard van de aandoening.[4]
In het werkgeversportaal worden onder meer de volgende gegevens verwerkt: de datum ingang ziekteverzuim, de datum beëindiging ziekteverzuim, ziek ten gevolge van zwangerschap, bevalling of orgaandonatie, de datum van de bevalling en de datum ingang zwangerschapsverlof.

40. Gelet op de aard van de persoonsgegevens worden in het werkgeversportaal derhalve gegevens betreffende iemands gezondheid verwerkt, hetgeen als een bijzondere categorie persoonsgegevens als bedoeld in artikel 9, eerste lid ,van de AVG wordt aangemerkt.

Verhoogd risico

41. In de Richtsnoeren Beveiliging van persoonsgegevens heeft de AP de eisen omtrent beveiliging uitgewerkt. De AP geeft aan dat bij bepaalde categorieën van persoonsgegevens de gevolgen van verlies of onrechtmatige verwerking ernstig kunnen zijn. Dit zijn de gegevens met een hoger of hoog risico. Onder deze categorieën vallen in ieder geval bijzondere persoonsgegevens.

[2] Zie ook CBP Richtsnoeren, Beveiliging van persoonsgegevens, februari 2013
[3] Zie met betrekking tot de risicoanalyse van UWV randnummer 54 en verder van dit besluit
[4] Kamerstukken II 1997/98, 25 892, nr. 3, p. 102

42. Daarnaast hanteert de AP de Handreiking versie 4[5]. Deze Handreiking geeft invulling aan de betrouwbaarheidsniveaus op basis van de eIDAS-verordening voor digitale identificatie- en vertrouwensdiensten[6], die vanaf 1 juli 2016 van kracht is (hierna: de eIDAS-verordening). De eIDAS-verordening onderscheidt drie betrouwbaarheidsniveaus van authenticatiemiddelen: laag, substantieel en hoog. De Handreiking biedt een classificatiemodel waarmee een vereenvoudigde risicoanalyse van de digitale dienst kan worden gemaakt. Het belangrijkste criterium hierbij is de aard van de te beschermen persoonsgegevens. Hierin worden vier klassen persoonsgegevens onderscheiden: klasse 0, I (basis), II (verhoogd risico) en III (hoog risico), waarbij gegevens met een verhoogd risico ook een hoger beveiligingsniveau vereisen.

43. De AP stelt vast dat de gegevens die in het werkgeversportaal verwerkt worden, volgens de Handreiking zogenaamde klasse II-persoonsgegevens zijn omdat het gaat om bijzondere persoonsgegevens. Voor klasse II-gegevens geldt een verhoogd risico.[7] Van een hoog risico, zoals bij de zogenoemde klasse III-gegevens, is gezien de aard van de gegevens die in het portaal worden verwerkt geen sprake.

Meerfactorauthenticatie

44. Op een verwerking van klasse II-gegevens is volgens de Handreiking minimaal betrouwbaarheidsniveau 'substantieel' van toepassing.[8] Ook bij de beantwoording van de vraag wat ten aanzien van dit betrouwbaarheidsniveau passende maatregelen zijn zoals bedoeld in artikel 32, eerste lid, van de AVG biedt de Handreiking een kader: zowel voor betrouwbaarheidsniveau 'substantieel' als betrouwbaarheidsniveau 'hoog' is, als type authenticatiemiddel, meerfactorauthenticatie vereist.[9]

45. De eis van meerfactorauthenticatie bij het verlenen van toegang tot een systeem waarin gezondheidsgegevens worden verwerkt wordt daarnaast onderschreven door beveiligingsstandaarden als NEN-7510, die aanwijzing geeft voor het toepassen van de Code voor informatiebeveiliging ISO/IEC 27002 in de gezondheidszorg:

[5] Een handreiking voor overheidsorganisaties: Betrouwbaarheidsniveaus voor digitale dienstverlening, versie 4, Forum Standaardisatie
[6] Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt
[7] Een handreiking voor overheidsorganisaties, versie 4, Forum voor Standaardisatie, p. 33
[8] Een handreiking voor overheidsorganisaties, versie 4, Forum voor Standaardisatie, p. 29. Het is mogelijk dat UWV na de risicoanalyse op basis van alle in de Handreiking versie 4 genoemde criteria uitkomt op betrouwbaarheidsniveau 'hoog' in plaats van 'substantieel'. Deze beoordeling zal UWV zelf moeten maken, zie ook randnummer 54 en verder.
[9] Een handreiking voor overheidsorganisaties, versie 4, Forum voor Standaardisatie, p. 24 – 25. Deze eis is neergelegd in de bijlage bij de Uitvoeringsverordening 2015/1502 van de Europese Commissie tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen overeenkomstig art. 8, lid 3, van de Verordening (EU) nr. 910/2014, waarop de Handreiking zich baseert.

'Gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, behoren de identiteit van gebruikers vast te stellen en dit behoort te worden gedaan door middel van authenticatie waarbij ten minste twee factoren betrokken worden.'[10]

46. Als passende maatregel zoals bedoeld in artikel 32, eerste lid, van de AVG moet bij het verlenen van toegang tot het werkgeversportaal zodoende gebruik worden gemaakt van meerfactorauthenticatie. Nu toegang tot het portaal plaatsvindt middels een vorm van éénfactorauthenticatie, handelt het UWV in strijd met artikel 32, eerste lid, van de AVG. UWV heeft dit ook erkend.

Overtreder

47. Het UWV is als overtreder aan te merken, omdat zij verwerkingsverantwoordelijke is in de zin van de AVG. Het UWV stelt het doel van en de middelen voor de verwerking van persoonsgegevens vast: het werkgeversportaal is een dienst van het UWV en wordt door het UWV ter beschikking gesteld aan werkgevers, waarbij de doeleinden van de gegevensverwerking door het UWV worden bepaald. Tevens heeft het UWV het in haar macht de overtreding te beëindigen.

De oplossing van het UWV: eHerkenning

48. Reeds bij brief van 25 januari 2016 heeft het UWV de overtreding van thans artikel 32, eerste lid, van de Wbp onderkend. Het UWV gaf hierbij aan voornemens te zijn om voor het werkgeversportaal gebruik te maken van eHerkenning, welke voorziening voorziet in het gebruik van meerfactorauthenticatie bij het verlenen van toegang tot het werkgeversportaal.

49. EHerkenning is een stelsel dat bedrijven elektronische toegang biedt tot de overheid en overheidsvoorzieningen. Ondernemers of medewerkers van een organisatie kunnen zich met één inlogmiddel veilig en eenvoudig identificeren bij verschillende organisaties. Overheidsorganisaties hoeven zelf geen eigen authenticatiesysteem te ontwikkelen maar kunnen op het stelsel aansluiten. De ontwikkeling van eHerkenning is een publiek-private samenwerking die onder regie staat van de ministeries van Economische Zaken en Klimaat en Binnenlandse Zaken en Koninkrijksrelaties. EHerkenning kent vijf verschillende betrouwbaarheidsniveaus. Bij deze betrouwbaarheidsniveaus is aansluiting gezocht bij de drie betrouwbaarheidsniveaus die de eIDAS-verordening onderscheidt en de eisen die bij die verordening aan de middelen worden gesteld. De overheidsorganisatie bepaalt zelf het betrouwbaarheidsniveau dat wordt toegepast.

50. Het UWV heeft aangegeven dat de invoering van eHerkenning door het UWV moet worden bezien in het licht van de Wdo die momenteel in voorbereiding is. De Wdo heeft als doel het veilig en betrouwbaar kunnen inloggen voor Nederlandse burgers en bedrijven bij de (semi-)overheid. Hiermee implementeert Nederland de EU richtlijn over toegankelijkheid van overheidswebsites en apps.[11] Vooruitlopend op de

[10] NEN-7510 (2017), p. 57
[11] https://www.digitaleoverheid.nl/voorzieningen/identificatie-en-authenticatie/eid/wet-gdi/.

Wdo is door de overheid eHerkenning ontwikkeld. Het UWV zal op termijn verplicht moeten aansluiten op eHerkenning.

51. Het UWV heeft aangegeven de implementatie van eHerkenning als enige reële oplossing te zien. Het UWV heeft mogelijke tussenoplossingen onderzocht, waarbij meerfactorauthenticatie met sms als tweede factor de meest haalbare en veilige alternatieve optie was. De technische implementatie hiervan zou echter net zo lang duren als de implementatie van eHerkenning en zou bovendien de implementatie van eHerkenning vertragen, omdat dit door hetzelfde team moet worden uitgevoerd. Daarnaast zou het niet doelmatig en proportioneel zijn om kort op elkaar twee ingrijpende implementatietrajecten te doorlopen: dit leidt tot extra administratieve lasten voor werkgevers en ondoelmatige inzet van publieke middelen.

Tijdsverloop/planning

52. Het UWV heeft aangegeven reeds in 2015 bezig te zijn geweest met het aansluiten op eHerkenning. Voor het UWV zijn echter de beschikbaarheid van het RSIN (Rechtspersonen en Samenwerkingsverbanden Informatienummer) en het BSN voor eenmanszaken in het stelsel van eHerkenning noodzakelijk, omdat zonder deze nummers het UWV eHerkenning niet kan koppelen aan haar systemen. Het UWV is voor deze uitbreiding van het stelsel afhankelijk van derden en heeft deze uitbreiding als voorwaarde gesteld voor de overstap op eHerkenning. In april 2017 heeft het UWV besloten de implementatie van eHerkenning op te starten omdat op dat moment zicht is op koppeling van het RSIN aan eHerkenning (87,7 % van de gebruikers van het werkgeverportaal wordt met RSIN geïdentificeerd). In haar zienswijze van 21 juni 2017 heeft het UWV aangegeven de aansluiting op eHerkenning naar verwachting in mei 2018 gerealiseerd te hebben. In november 2017 rondt het UWV het vooronderzoek af. In februari 2018 heeft het UWV het projectplan eHerkenning werkgeversportaal vastgesteld en op verzoek van de AP de AP doen toekomen.

53. Volgens dit projectplan koerst het UWV op 1 november 2018 als implementatiedatum, met vervolgens een uitrolperiode van een jaar waarin de gebruikers van het portaal kunnen overstappen. Op de hoorzitting heeft het UWV aangegeven nu uit te gaan van implementatie in het vierde kwartaal van 2018. Naar verwachting wordt in de tweede helft van 2018 ook het BSN aan het stelsel toegevoegd. Voor deze groep geldt dezelfde implementatiedatum met uitrolperiode. Er is ook nog een groep gebruikers (0,7%) die geen gebruik kan maken van eHerkenning en waarvoor nog geen oplossing beschikbaar is. Het UWV heeft aangegeven dat indien er geen oplossing komt, deze groep per 1 november 2019 geen gebruik meer kan maken van het werkgeversportaal.

Betrouwbaarheidsniveau; toepassing Handreiking versie 4

54. In 2015 heeft het UWV aan de hand van de toen beschikbare Handreiking van Forum standaardisatie, versie 3[12] een risicoanalyse gedaan. Deze versie van de handreiking is gebaseerd op het Europese

[12] Een handreiking voor overheidsorganisaties: betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten, versie 3, Forum Standaardisatie

STORKraamwerk. Uit deze risicoanalyse kwam naar voren dat niveau STORK 3 passend is.
Het UWV heeft de AP deze risicoanalyse op verzoek bij brief van3 april 2018 doen toekomen.

55. In november 2016 is versie 4 van de Handreiking verschenen. Deze versie baseert zich niet meer op het STORK-raamwerk maar, zoals eerder weergegeven, op de eIDAS-verordening. Het UWV heeft hierin echter geen aanleiding gezien om de risicoanalyse van 2015 opnieuw tegen het licht te houden aan de hand van de nieuwste versie van de Handreiking. In haar brief van 25 mei 2018 geeft het UWV aan dat in de risicoanalyse van 2015 UWV het eIDAS-stelsel heeft meegenomen als voorgenomen wetgeving.
De nieuwe versie van de Handreiking heeft derhalve 'geen aanleiding gegeven om een nieuwe risicoanalyse uit te voeren'.

56. Blijkens het projectplan eHerkenning werkgeversportaal heeft het UWV gekozen voor aansluiting op eHerkenning-niveau 3. Dit komt overeen met eIDAS-niveau substantieel.

57. De AP stelt vast dat de risicoanalyse van het UWV uit 2015 gebaseerd is op versie 3 van de Handreiking. De norm uit artikel 32, eerste lid, van de AVG , en voorheen artikel 13 van de Wbp, schrijft voor dat de (verwerkings)verantwoordelijke bij het treffen van passende technische en organisatorische maatregelen teneinde een passend beveiligingsniveau te waarborgen, onder meer rekening houdt met de stand van de techniek. Hierin ligt onder meer besloten dat een reeds gedane risicobeoordeling van tijd tot tijd opnieuw moet worden geactualiseerd aan de hand van de op dat moment geldende standaarden. Het had dan ook op de weg van het UWV gelegen om de reeds in 2015 uitgevoerde risicoanalyse opnieuw uit te voeren aan de hand van de meest recente versie van de Handreiking. Door dit niet te doen ontstaat het risico dat aan het einde van de implementatietermijn van, in dit geval, eHerkenning, mogelijk geen sprake (meer) is van een passend beveiligingsniveau.

58. Hoewel betrouwbaarheidsniveau Stork 3 uit versie 3 van de Handreiking overeen lijkt te komen met e-IDAS betrouwbaarheidsniveau substantieel uit versie 4 van de Handreiking, hanteren beide versies van de Handreiking verschillende toetsingskaders. Toetsing aan versie 4 van de Handreiking leidt daardoor mogelijk tot de uitkomst dat van een hoger betrouwbaarheidsniveau moet worden uitgegaan dan het UWV tot nu toe op grond van versie 3 van de Handreiking heeft gedaan. Uiteindelijk is dit bepalend voor de keuze van de maatregelen die getroffen moeten worden om een passend beveiligingsniveau te waarborgen. De AP kan niet voor of in de plaats van het UWV alle uit Handreiking versie 4 relevante factoren beoordelen.

Last onder dwangsom en begunstigingstermijn

59. Uit artikel 16, eerste lid, van de UAVG, in samenhang bezien met artikel 5:32, eerste lid, van de Awb volgt dat de AP bevoegd is om een last onder dwangsom op te leggen bij overtreding van artikel 32, eerste lid van de AVG. Ingevolge artikel 5:2, eerste lid, onder b, van de Awb kan de last gericht zijn op het beëindigen van de geconstateerde overtreding en het voorkomen van herhaling.

60. De AP gelast het UWV om binnen de begunstigingstermijn van het besluit de overtreding van artikel 32, eerste lid, van de AVG te beëindigen. Dit betekent dat het UWV binnen de begunstigingstermijn maatregelen moet nemen die zorgen voor een passend beveiligingsniveau met betrekking tot het verlenen van toegang tot het werkgeversportaal, waarbij inloggen alleen mogelijk is middels een passende vorm van meerfactorauthenticatie (bijvoorbeeld door gebruik van eHerkenning). Omdat het UWV bij het bepalen van het betrouwbaarheidsniveau voor het werkgeversportaal gebruik heeft gemaakt van een inmiddels verouderde versie van de Handreiking, dient het UWV het betrouwbaarheidsniveau hierbij opnieuw te bepalen door een risicoanalyse uit te voeren aan de hand van versie 4 van de Handreiking.

61. Artikel 5:32a, tweede lid, van de Awb bepaalt dat een begunstigingstermijn wordt gesteld 'gedurende welke de overtreder de last kan uitvoeren zonder dat een dwangsom wordt verbeurd'. De termijn gedurende welke een last kan worden uitgevoerd zonder dat een dwangsom wordt verbeurd, moet zo kort mogelijk worden gesteld. De termijn moet wel lang genoeg zijn om de last te kunnen uitvoeren.

62. Gelet op het vorenstaande besluit de AP dat het UWV uiterlijk op **31 oktober 2019** aan de last moet voldoen. De AP heeft bij het vaststellen van de begunstigingstermijn rekening gehouden met de planning van het UWV ten aanzien van de implementatie van eHerkenning en de daarin genoemde uitrolperiode van een jaar na implementatie op 1 november 2018.

63. Artikel 5:32b, derde lid, van de Awb schrijft voor dat de dwangsombedragen in redelijke verhouding staan tot de zwaarte van het geschonden belang en tot de beoogde werking van de dwangsom. Bij dat laatste is van belang dat van een dwangsom een zodanige prikkel moet uitgaan dat aan de last wordt voldaan.

64. Indien het UWV niet binnen de begunstigingstermijn de geconstateerde overtreding beëindigt, verbeurt zij een dwangsom. De AP stelt de hoogte van deze dwangsom vast op € 150.000,- voor iedere maand dat de last niet (geheel) is uitgevoerd tot een maximum van € 900.000,-. Naar het oordeel van de AP staat de hoogte van deze bedragen in redelijke verhouding tot de zwaarte van het door de overtreding geschonden belang – de bescherming van bijzondere persoonsgegevens en van de persoonlijke levenssfeer van betrokkenen – en zijn deze voorts voldoende hoog om UWV te bewegen de overtreding te beëindigen. Daarbij betrekt de AP de kosten die aan de implementatie van eHerkenning zijn gekoppeld, als ook de structurele meerkosten per jaar.

65. De AP verzoekt het UWV tijdig **vóór 1 oktober 2018** de opnieuw uitgevoerde risicoanalyse waarin het UWV aan het werkgeversportaal een betrouwbaarheidsniveau toekent, toe te zenden. Dit laat overigens onverlet dat de AP bevoegd is om een onderzoek, waaronder een onderzoek ter plaatse, in te stellen indien haar dit dienstig voorkomt.

Datum
31 juli 2018

Ons kenmerk
z2018-02009

Dictum

De AP legt aan het UWV, wegens overtreding van artikel 32, eerste lid, van de AVG, een last onder dwangsom op met de volgende inhoud:

- Het UWV dient uiterlijk op 31 oktober 2019 het verlenen van toegang tot het werkgeversportaal van een passend beveiligingsniveau te voorzien, waarbij inloggen vanaf dat moment alleen mogelijk is middels een passende vorm van meerfactorauthenticatie. Voorafgaand hieraan dient Het UWV het vereiste betrouwbaarheidsniveau opnieuw te bepalen door een risicoanalyse uit te voeren aan de hand van versie 4 van de Handreiking.

-Het UWV verbeurt na afloop van deze termijn een dwangsom van € 150.000,- (zegge: honderdvijftigduizend euro) voor iedere maand dat de last niet (geheel) is uitgevoerd tot een maximum van € 900.000,- (zegge: negenhonderdduizend euro).

De Autoriteit Persoonsgegevens,
Namens deze,

w.g.

Mr. A. Wolfsen
Voorzitter

Indien u het niet eens bent met dit besluit kunt u binnen zes weken na de datum van verzending van het besluit een bezwaarschrift indienen bij de Autoriteit Persoonsgegevens, Postbus 93374, 2509 AJ Den Haag, onder vermelding van “Awb-bezwaar” op de envelop.