Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2018–2019

32 761 Verwerking en bescherming persoonsgegevens

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 127

BRIEF VAN DE MINISTER VAN SOCIALE ZAKEN EN WERKGELEGENHEID

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 26 november 2018

Conform het verzoek van de vaste commissie voor Sociale Zaken en Werkgelegenheid van 30 oktober jl. stuur ik u hierbij een reactie op het bericht in het Algemeen Dagblad van 30 oktober 2018 inzake de oplegging van een last onder dwangsom door de Autoriteit Persoonsgegevens aan UWV in verband met de beveiliging van het werkgeversportaal. Ook ga ik in op de stand van zaken van de maatregelen die door UWV zijn genomen naar aanleiding van datalekken in het verleden.

Beveiliging werkgeversportaal

In deze brief informeer ik u over het onderzoek door de Autoriteit Persoonsgegevens en de maatregelen die UWV heeft genomen en nog zal nemen om de authenticatie op het werkgeversportaal te verbeteren. Voordat ik daarop in ga wil ik benadrukken dat ik de uitkomsten van het onderzoek van de Autoriteit Persoonsgegevens volledig onderschrijf: het is van groot belang dat (bijzondere) persoonsgegevens van burgers op het juiste niveau zijn beveiligd tegen ongeautoriseerde toegang. Ook UWV neemt deze bescherming serieus en is sinds de geconstateerde bevinding in gesprek met de Autoriteit Persoonsgegevens over de wijze waarop en de termijn waarbinnen UWV zal en kan voldoen aan de eisen die de privacywetgeving stelt.

Werkgeversportaal

Via het werkgeversportaal biedt het UWV een aantal onlinediensten aan waarmee de administratieve en papieren last bij werkgevers wordt verminderd. Zo biedt het portaal onder andere de mogelijkheid voor werkgevers tot het invoeren en bekijken van ziekteverzuimgegevens van medewerkers, het uploaden van re-integratieverslagen, het indienen van ontslagaanvragen, het raadplegen van het doelgroepregister in het kader van de Banenafspraak, het doorgeven van wijzigingen en het inzien van

kst-32761-127
ISSN 0921 - 7371
's-Gravenhage 2018

brieven in het kader van de Ziektewet en de Wet Arbeid en Zorg (WAZO) en bevat het portaal informatie voor eigenrisicodragers.

Er zijn ca. 157.000 werkgevers en ca. 2.700 intermediairs (zoals arbodiensten, administratiekantoren of accountants) die geautoriseerd zijn voor ruim 25.000 werkgevers, die beschikken over een toegangsaccount voor het werkgeversportaal. In 2017 is er in totaal ruim 1,2 miljoen keer ingelogd op het portaal.

Onderzoek Autoriteit Persoonsgegevens

In juni 2015 heeft de Autoriteit Persoonsgegevens naar alle (bekende) beheerders van verzuimsystemen een brief gestuurd waarin is aangegeven aan welke wettelijke eisen die voortvloeien uit de (toen geldende) Wet bescherming persoonsgegevens die systemen moeten voldoen. Daarbij zijn twee concrete beveiligingseisen genoemd:

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

In november 2015 heeft de Autoriteit Persoonsgegevens UWV per brief erop gewezen dat deze eisen ook gelden ten aanzien van het werkgeversportaal.

UWV heeft in januari 2016 per brief aan de Autoriteit Persoonsgegevens bevestigd dat de authenticatie voor het werkgeversportaal inderdaad niet voldoet aan de eisen van de Wet bescherming persoonsgegevens en aangegeven dat UWV dit niveau wil verhogen met de implementatie van de rijksbrede voorziening eHerkenning. UWV heeft laten weten daar onderzoek naar te doen, maar dat de toepassing daarvan nog op een probleem stuit, omdat het Rechtspersonen en Samenwerkingsverbanden Informatienummer (RSIN) op dat moment nog niet in het stelsel van eHerkenning was opgenomen, terwijl dit nummer noodzakelijk is voor de identificatie van werkgevers.

UWV heeft vervolgens de mogelijkheden onderzocht om via een alternatieve, tijdelijke voorziening tweefactorauthenticatie in te voeren, bijvoorbeeld via een sms-service. Hieruit bleek dat de invoering van een dergelijke tijdelijke voorziening in 2017 niet realistisch was. Tevens achtte UWV het vanuit dienstverleningsperspectief ongewenst om werkgevers kort op elkaar twee keer een implementatietraject voor een authenticatiemiddel te laten doorlopen, aangezien UWV ook een aansluiting op eHerkenning wilde realiseren. Aansluiting op eHerkenning was ook onderdeel van de toen op handen zijnde Wet Generieke Digitale Infrastructuur (nu: Wet Digitale Overheid).

Begin 2017 werd bekend dat het RSIN zou worden gekoppeld aan eHerkenning, waarna is besloten om te starten met de voorbereidingen van de implementatie van eHerkenning op het werkgeversportaal. Op dat moment kon UWV nog geen concrete planning afgeven voor de realisatie. Dit was voor de Autoriteit Persoonsgegevens aanleiding om in het kader van haar toezichthoudende taak een ambtshalve onderzoek in te stellen naar de naleving van de Wet bescherming persoonsgegevens, in het bijzonder het gebruik van meerfactorauthenticatie bij de toegang tot het werkgeversportaal van UWV.

Conclusie van het onderzoek van de Autoriteit Persoonsgegevens is dat UWV geen meerfactorauthenticatie toepast bij het verlenen van toegang

tot het werkgeversportaal, terwijl dat gelet op de aard van de gegevens (verzuimgegevens zijn gegevens betreffende de gezondheid) wel noodzakelijk is. Ook heeft UWV er niet op een andere manier zorg voor gedragen dat passende maatregelen waren getroffen voor het verkrijgen van toegang tot de gegevens in het portaal. Hiermee handelt UWV in strijd met de Wet bescherming persoonsgegevens, die sinds 25 mei 2018 is vervangen door de Algemene verordening gegevensbescherming.

Gelet op het voortduren van de overtreding heeft de Autoriteit Persoonsgegevens op 31 juli 2018 een last onder dwangsom opgelegd. De last houdt in dat UWV uiterlijk op 31 oktober 2019 het verlenen van toegang tot het werkgeversportaal van een passend beveiligingsniveau dient te voorzien, waarbij inloggen vanaf dat moment alleen nog mogelijk is via een passende vorm van meerfactorauthenticatie. Tevens dient UWV voorafgaand hieraan het vereiste beveiligingsniveau opnieuw te bepalen door een risicoanalyse uit te voeren aan de hand van de meest recente versie van de daarvoor geldende overheidshandreiking[1]. De hoogte van de dwangsom bedraagt 150.000 euro voor iedere maand dat de last niet (geheel) is uitgevoerd, met een maximum van 900.000 euro.

Maatregelen UWV

Naar aanleiding van de geconstateerde overtreding heeft UWV zoals hierboven geschetst in 2017 verschillende mogelijkheden onderzocht en gekozen voor de implementatie van eHerkenning als meerfactorauthenticatie voor het werkgeversportaal. Ik steun die keuze. Daarmee sluit UWV aan bij de ontwikkeling van het overheidsbrede authenticatiestelsel voor bedrijven en anticipeert UWV op de inwerkingtreding van de Wet Digitale Overheid die ter behandeling bij uw Kamer voorligt. Door te kiezen voor deze vorm van meerfactorauthenticatie wordt tevens voorkomen dat werkgevers binnen een relatief korte periode twee keer een nieuw authenticatiemiddel moeten aanschaffen en inregelen. Het authenticatiemiddel dat werkgevers moeten aanschaffen voor het werkgeversportaal kan nu en vooral in de toekomst ook worden gebruikt voor alle andere online-overheidsdiensten.

UWV is de eerste overheidsinstantie die op grote schaal eHerkenning op betrouwbaarheidsniveau 3 (substantieel) inzet voor de onlinedienstverlening aan bedrijven. Dit betekent dat UWV ook te maken krijgt met een aantal kinderziektes binnen het eHerkenningsstelsel, waardoor enige vertraging is opgetreden in de geplande implementatie. Daarnaast werkt het publiek-private stelsel van eHerkenning zodanig dat UWV afhankelijk is van andere partijen voor het doorvoeren van wijzigingen. Dit maakt ook dat UWV beperkt rechtstreeks invloed kan uitoefenen op noodzakelijke ontwikkelingen binnen het stelsel. Dit heeft invloed gehad op de (doorlooptijd van de) implementatie van eHerkenning bij UWV. Op dit moment kan UWV nog niet alle doelgroepen werkgevers met eHerkenning bedienen.[2] Op 22 november jl. heeft UWV eHerkenning in gebruik genomen op het werkgeversportaal. Werkgevers die gebruik willen (blijven) maken van het portaal hebben tot 1 november 2019 de tijd om eHerkenningsmiddelen aan te schaffen. Vanaf die datum zal het voor werkgevers niet meer mogelijk zijn om met hun huidige inloggegevens toegang te krijgen tot de diensten op het werkgeversportaal. Momenteel loopt er een online media campagne vanuit het Ministerie van Binnen-

[1] Een handreiking voor overheidsorganisaties: betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten, versie 4, Forum Standaardisatie.
[2] Dit betreft zelfstandigen met personeel en werkgevers zonder inschrijving bij de Kamer van Koophandel.

landse Zaken en Koninkrijksrelaties om meer bekendheid te geven aan eHerkenning.[3]

UWV implementeert eHerkenning op betrouwbaarheidsniveau 3 (substantieel). Uit de risicoanalyse die UWV heeft uitgevoerd aan de hand van de nieuwste daarvoor geldende overheidshandreiking blijkt dat dit niveau een passend beveiligingsniveau is voor de verzuimmelder op het werkgeversportaal. Hiermee borgt UWV dat de toegang tot de gegevens in de verzuimmelder op het gewenste niveau met meerfactorauthenticatie beveiligd is.

In afwachting van de ingebruikname van eHerkenning heeft UWV verschillende extra maatregelen getroffen om de toegang door onbevoegden tot het werkgeversportaal tegen te gaan. Standaard vindt er binnen UWV preventie, logging en monitoring plaats, zowel op het niveau van de infrastructuur als op het niveau van de applicaties. Ook voert UWV periodiek securityscans en penetratietesten uit om te testen of applicaties aan de beveiligingsrichtlijnen voldoen en om een instabiel UWV-netwerk te voorkomen. Tot heden zijn er bij UWV geen signalen van misbruik via het werkgeversportaal gemeld.

Met monitoring worden pogingen gedetecteerd van personen die op een niet-toegestane manier de UWV systemen en gegevens via het werkgeversportaal proberen te bereiken. Logging en monitoring is ingeregeld om ervoor te zorgen dat high risk/impact security incidenten voorkomen worden en indien nodig met prioriteit worden afgehandeld. De applicatielogging en infrastructuurlogging zijn beiden specifiek voor het werkgeversportaal uitgebreid. Bij vermoedens van misbruik worden technische forensische onderzoeken uitgevoerd. Er is een continue rapportage- en verbetercyclus ingericht. Zo kan UWV snel reageren wanneer misbruik wordt gedetecteerd.

Stand van zaken datalekken

Burgers moeten erop kunnen vertrouwen dat er zorgvuldig met hun persoonsgegevens wordt omgegaan. Datalekken moeten zoveel mogelijk worden voorkomen, maar zijn helaas nooit volledig uit te sluiten. Zoals ik ook in mijn antwoorden van 24 september 2018 op de vragen van het lid Kent (SP) over de berichtgeving inzake een datalek bij UWV heb aangegeven (Aanhangsel Handelingen II 2018/19, nr. 51), blijven onderdelen van het werkproces bij UWV mensenwerk en is de kans op datalekken helaas nooit volledig uit te sluiten. Dat risico moet echter zoveel mogelijk worden beperkt. Om die reden is het essentieel dat UWV ondersteunende en technische maatregelen neemt die medewerkers helpen in hun werk en de kans op datalekken en de potentiële omvang daarvan minimaliseren. Een beperkende factor daarin is dat veranderingen in de ICT-systemen van UWV complex en tijdrovend zijn. Ook geldt dat technische maatregelen niet in elke situatie of in elk systeem toepasbaar zijn. Dit mag geen excuus zijn om geen verbeteringen na te streven, maar betekent wel dat het gebruik van oudere systemen gevoeliger blijft voor menselijke fouten.

UWV heeft naar aanleiding van een datalek in 2016 allereerst tijdelijke maatregelen getroffen, zoals het niet langer verzenden van bulkberichten en het niet langer verzenden van e-mails via Outlook. Vervolgens heeft UWV meer structurele maatregelen getroffen tegen datalekken, waaronder het opstellen van de richtlijn veilig communiceren en het verzorgen van een workshop preventie datalekken in alle districten in

[3] https://www.eherkenning.nl/nieuws/item/artikel/eherkenning-in-de-schijnwerpers/.

2017.[4] Naar aanleiding van de uitkomsten van het onderzoek zijn er verschillende verbetermaatregelen in gang gezet, vooral gericht op het verbeteren van het bewustzijn van medewerkers en op verbetering van werkprocessen. Daarnaast heeft het onderzoek een technische maatregel opgeleverd met betrekking tot het blokkeren van de mogelijkheid tot het uploaden van bepaalde bestanden. Deze maatregel zal in het tweede kwartaal 2019 worden ingevoerd.

Naar aanleiding van het datalek in augustus 2018 heb ik UWV verzocht om meer technische maatregelen te onderzoeken en te nemen die het menselijk handelen kunnen ondersteunen en het risico op datalekken kunnen verkleinen, zoals extra verificatiestappen, technische blokkades en automatische waarschuwingen. Ook heb ik UWV gevraagd om strikter toe te zien op naleving van de bestaande werkprocedures en blijvend aandacht te geven aan een veilige omgang met persoonsgegevens.

De Minister van Sociale Zaken en Werkgelegenheid,
W. Koolmees

[4] Naast genoemde maatregelen zijn ambassadeurs veilige communicatie aangesteld, is er meer aandacht voor veilige omgang met gegevens in het integriteitsbeleid en worden gegevensbestanden opgeknipt in kleine delen.