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

Vertrouwelijk/Aangetekend
UWV
Raad van Bestuur
t.a.v. dhr. M.R.P.M. Camps
Postbus 58285
1040 HG
AMSTERDAM

Datum
31 mei 2021

Ons kenmerk
[VERTROUWELIJK]

Contactpersoon
[VERTROUWELIJK]

Onderwerp
Besluit tot het opleggen van een boete

Geachte heer Camps,

De Autoriteit Persoonsgegevens (AP) heeft besloten om aan het Uitvoeringsinstituut werknemersverzekeringen (UWV) een **bestuurlijke boete** van **€ 450.000** op te leggen. UWV heeft onvoldoende een op risico afgestemd beveiligingsniveau gegarandeerd en gewaarborgd in het kader van het verzenden van groepsberichten via de Mijn Werkmap-omgeving. Hierdoor heeft UWV in strijd gehandeld met artikel 13 van de Wet bescherming persoonsgegevens en artikel 32, eerste en tweede lid, van de Algemene verordening gegevensbescherming.

De AP licht het besluit hierna nader toe. Hoofdstuk 1 betreft een inleiding en hoofdstuk 2 bevat de feiten. De AP beoordeelt in hoofdstuk 3 of er sprake is van verwerking van persoonsgegevens, de verwerkingsverantwoordelijkheid en de overtreding. In hoofdstuk 4 wordt de (hoogte van de) bestuurlijke boete uitgewerkt en hoofdstuk 5 bevat het dictum en de rechtsmiddelenclausule.

1. Inleiding

1.1 Betrokken overheidsinstantie

Dit besluit heeft betrekking op het Uitvoeringsinstituut werknemersverzekeringen (hierna: UWV). Sinds augustus 2016 hebben bij UWV negen datalekken plaatsgevonden die soortgelijk van aard waren. De datalekken vonden allemaal plaats bij het versturen van een groepsbericht aan een groep werkzoekenden. Daarbij werd een verkeerd (Excel-)bestand met een veelheid aan gevoelige en bijzondere persoonsgegevens van een variërend aantal werkzoekenden meegezonden die zo in de 'Mijn Werkmap'-omgeving van werkzoekenden terecht kwam. Het aantal werkzoekenden van wie gegevens tussen 2016 en 2018 zijn gelekt, liep per datalek uiteen van 10 tot 11.062 personen.

Omdat in een periode van twee jaar negen soortgelijke datalekken hadden plaatsgevonden ondanks dat UWV had aangegeven dat zij maatregelen had getroffen, bestond het vermoeden dat UWV geen passende technische en organisatorische maatregelen (zoals de wet voorschrijft) had getroffen om tot een passend beveiligingsniveau te komen waardoor nieuwe gelijksoortige datalekken konden worden voorkomen. Daarom is de AP een ambtshalve onderzoek gestart. Dit besluit heeft betrekking op de periode van 2012 tot en met 2018.

1.2 Procesverloop

Op 4 september 2018 heeft een toezichthouder van de AP telefonisch contact opgenomen met de functionaris gegevensbescherming (hierna: FG) van UWV. Toezichthouders van de AP hebben vervolgens meermaals informatie opgevraagd bij UWV waarop UWV deze informatie heeft geleverd. UWV heeft ook op eigen initiatief nadere stukken aan de AP toegestuurd.

Op 31 oktober 2019 is UWV gevraagd te reageren op de feiten zoals die tot dan toe bekend waren bij de AP. Op 14 en 18 november 2019 heeft UWV op dat verzoek gereageerd. Bij brief van 11 maart 2021 heeft de AP aan het UWV een voornemen tot handhaving verzonden. Daartoe tevens bij deze brief door de AP in de gelegenheid gesteld, heeft het UWV op 8 en 19 april schriftelijk een zienswijze gegeven over dit voornemen en het daaraan ten grondslag gelegde rapport met bevindingen.

2. Feiten

2.1 Taken UWV en communicatie met werkzoekenden

UWV is ingesteld op grond van artikel 2, eerste lid, van de Wet structuur uitvoeringsorganisatie werk en inkomen (SUWI). UWV is een zelfstandig bestuursorgaan[1] met eigen rechtspersoonlijkheid.[2]

Binnen UWV houdt de divisie WERKbedrijf zich bezig met arbeidsbemiddeling en re-integratie. Dit doet zij door vraag en aanbod bij elkaar te brengen. Het WERKbedrijf richt zich primair op werkzoekenden met een grote afstand tot de arbeidsmarkt en op werkgevers die deze werkzoekenden willen aannemen. Personen die een uitkering op basis van de Werkeloosheidswet willen aanvragen, dienen zich bij UWV te registreren als werkzoekende.[3]

Werk.nl is een website van UWV. Sinds 2007 heeft iedere werkzoekende op werk.nl een persoonlijke omgeving die hem/haar helpt bij het zoeken naar een baan: Mijn Werkmap.[4] Indien een werkzoekende een uitkering heeft, kan deze via Mijn Werkmap onder andere wijzigingen, taken en sollicitatieactiviteiten doorgeven en berichten met bijlagen uitwisselen met UWV.[5]

UWV kan gebruik maken van groepsberichten als men hetzelfde bericht naar meerdere werkzoekenden moet verzenden. Deze UWV-berichten komen in de Mijn Werkmap-omgeving van werkzoekenden terecht.

2.2 Bronsysteem met opgeslagen gegevens werkzoekenden: Sonar

Sonar is het belangrijkste bronsysteem dat het WERKbedrijf en gemeenten gebruiken om werkzoekenden naar werk te bemiddelen door werkzoekenden aan vacatures bij werkgevers te koppelen.[6] Het systeem bevatte in de jaren 2016 tot en met 2018 gegevens over gemiddeld 4.500.000 personen, waaronder werkzoekenden, zieken en arbeidsongeschikten.[7]

Sonar bevat 630 gegevensvelden met daarin allerlei soorten gegevens van personen. Niet voor iedere persoon zijn alle gegevensvelden ingevuld.[8] De gegevens in Sonar betreffen onder meer NAW, opleiding(sniveau), nationaliteit, BSN, gegevens over fysieke beperkingen, psychisch en lichamelijk werkvermogen en of mensen zich te ziek voelen of te ziek zijn om te werken. Voor wat betreft sommige van

[1] Zie o.m. artikel 4 lid 1 SUWI en het zbo-register van de Nederlandse Rijksoverheid.
[2] Zie artikel 2 lid 2 SUWI en artikel 4 lid 1 SUWI en het zbo-register van de Nederlandse Rijksoverheid.
[3] Zie artikel 26, lid 1, onder b, d en e, Werkeloosheidswet.
[4] Zie o.a. dossierstuk 98 (Beantwoording door UWV, bestand "Aanvullende vragen AP2110", p. 1).
[5] Zie o.a. dossierstuk 120 (Pagina's website werk.nl 'Handleiding: Werkmap gebruiken').
[6] Zie o.a. dossierstuk 6 (Presentatie Programmaraad over UWV applicaties, p. 2, 3, 6 en 11).
[7] Zie dossierstuk 38 (Excel-bestand, antwoord op vraag 6 bij datalek 1) en dossierstuk 98 (Beantwoording door UWV, bestand "Aanvullende vragen AP2110", p. 1).
[8] Zie dossierstuk 38 (Excel-bestand, antwoord op vraag 6 bij datalek 1) en dossierstuk 81 (Beantwoording door UWV, bijlage 1 (bestand "Beantwoording vragen AP augustus 2019", antwoord op vraag 9) en bijlage 4 (bestand "Vraag 9 - bijlage")).

deze gegevens kan het gaan om de gemoedstoestand of perceptie van de werkzoekende, die zelf een online vragenlijst heeft ingevuld.[9]

Sonar heeft ongeveer 15.000 gebruikers. De helft van het totaal aantal accounts is van het WERKbedrijf en gemeenten en de andere helft is van andere divisies binnen UWV. Alle gebruikers hebben de mogelijkheid zoekopdrachten te maken en op te slaan. Gebruikers hebben op basis van functie en bijbehorende taken toegang tot deze gegevens.[10]

2.3 Groepsberichten

De directie van het WERKbedrijf heeft op 16 juli 2012, na datalekken via de e-mail, de groepsberichtenfunctionaliteit in Sonar verplicht gesteld voor het versturen van groepsberichten naar meerdere werkzoekenden tegelijk.[11] Tevens is toen besloten dit besluit samen met de Quick Reference Card "*Sonar groepsmail verzenden naar de werkmap*" dwingend onder de aandacht van de uitvoerende medewerkers van UWV te brengen.[12] Een Quick Reference Card wordt door UWV binnen het WERKbedrijf gebruikt voor het vastleggen van procedures en het richting UWV-medewerkers communiceren van deze procedures.

Er zijn bepaalde handelingen nodig om via Sonar een groepsbericht of een uitnodiging aan een selectie werkzoekenden te versturen.[13] Allereerst selecteert een medewerker van UWV een bepaalde groep personen in Sonar en vraagt soorten gegevens over hen op in Sonar. Vervolgens exporteert de medewerker van UWV deze set met gegevens van specifieke personen uit Sonar en slaat deze geëxporteerde gegevens op. Daarna worden deze gegevens omgezet in een Excel/csv-bestand. Er is geen limiet op het aantal personen wiens gegevens kunnen worden geëxporteerd. Bovendien worden de bestanden niet beveiligd, omdat dit volgens UWV de uitvoering zou bemoeilijken.[14] Vervolgens wordt dit bestand gebruikt als basis om de geadresseerden van het groepsbericht te bepalen.[15] Het groepsbericht komt na verzending door het UWV vervolgens bij de geadresseerden in de Mijn Werkmap-omgeving. Dit proces voor het verspreiden van een groepsbericht beschrijft UWV aldus in de Quick Reference Card "*Sonar Verzenden groepsberichten vanuit Sonar naar de werkmap*" (hierna: QRC groepsberichten).[16]

---

[9] Zie dossierstuk 38 (Excel-bestand, antwoord op vraag 2 bij datalekken 1 t/m 7) en dossierstuk 81 (Beantwoording door UWV, bijlage 1 (bestand "Beantwoording vragen AP augustus 2019", antwoord op vraag 3) en bijlage 2 (bestand "Vraag 3 - bijlage")).
[10] Zie o.a. dossierstuk 81 (Beantwoording door UWV, bijlage 1 (bestand "Beantwoording vragen AP augustus 2019", antwoord op vraag 10)).
[11] Zie o.a. dossierstuk 98 (Beantwoording door UWV, bestand "Aanvullende vragen AP2110", p. 3 en bijlage 6 (bestand "29-12 actiepuntenlijst DT", p. 3 onder punt 4)).
[12] Zie dossierstuk 98 (Beantwoording door UWV, bestand "Aanvullende vragen AP2110", p. 2 en bijlage 4 (bestand "28 BV 06 Oplegger verbieden Outlook groepsberichten 0406212") en bijlage 5 (bestand "28 BV 06 Beslisdocument verbieden gebruik groepsmail via Outlook")).
[13] Zie dossierstuk 66 (Beantwoording door UWV, p. 3).
[14] Zie dossierstuk 38 (Excel-bestand, bij "Korte omschrijving" m.b.t. alle datalekken) en dossierstuk 81 (Beantwoording door UWV, bijlage 1 (bestand "Beantwoording vragen AP augustus 2019", antwoord vraag 11)).
[15] Zie dossierstuk 81 (Beantwoording door UWV, bijlage 1 (bestand "Beantwoording vragen AP augustus 2019", antwoord vraag 11)).
[16] Zie dossierstuk 38 (Excel-bestand, bijlage 29 (bestand "Microsoft Word 97-1003-document" met toelichting bij antwoord op vraag 13 bij datalek 6 en 7)), dossierstuk 91 (Beantwoording door UWV, bijlagen 1 t/m 4).

Volgens UWV is er bij het verzenden van een groepsbericht wel een beperking op het aantal personen aan wie het bericht kan worden verzonden.[17] Sinds medio 2013 tot heden is dit aantal beperkt tot 100 om de technische problemen in Sonar te voorkomen, waardoor de werking en stabiliteit daarvan verbetert en het berichtenverkeer soepeler verloopt.[18] In alle gebruikte versies van de QRC groepsberichten staat dat indien een UWV-medewerker toch meer dan 100 personen wil benaderen via de Mijn Werkmap-omgeving, dit bij het Functioneel Beheer kan worden aangevraagd. Functioneel Beheer kan het maximum zeer tijdelijk ophogen naar een groter aantal personen.[19] Verder staat in de QRC groepsberichten dat er bijlagen kunnen worden meegezonden met groepsberichten via Sonar, maar dat het de voorkeur heeft dit niet te doen.[20]

In de periode van januari 2016 tot en met september 2018 zijn volgens UWV in totaal 61.214 groepsberichten via de Mijn Werkmap-omgeving verstuurd, met een gemiddelde van 215 geadresseerde personen per groepsbericht.[21]

2.4 Datalekken met betrekking tot de groepsberichten

In totaal hebben er sinds begin 2016 negen datalekken plaatsgevonden gerelateerd aan de persoonlijke omgeving van werkzoekenden: Mijn Werkmap.[22] UWV heeft acht van deze datalekken gemeld bij de AP.[23] Voor 1 januari 2016 bestond er geen verplichting om datalekken te melden bij de AP.

Bij deze datalekken is bij het aanmaken van het groepsbericht steeds het Excel-bestand met de export uit Sonar toegevoegd. Hierdoor kwam dit bestand met de export (in plaats van een bericht dat verzonden had moeten worden zoals bijvoorbeeld een vacaturetekst) in de Mijn Werkmap-omgeving van werkzoekenden terecht. Zodoende kon het niet beveiligde en te raadplegen bestand met de individuele gegevens over alle geadresseerden van het bericht terechtkomen bij alle beoogde geadresseerden.[24]

De AP heeft in de tabel hieronder de belangrijkste feiten over de negen datalekken weergegeven.[25]

[17] Zie dossierstuk 81 (Beantwoording door UWV, bijlage 1 (bestand "Beantwoording vragen AP augustus 2019", antwoord vraag 11)).
[18] Zie dossierstuk 91 (Beantwoording door UWV, bijlagen 1 t/m 4).
[19] Zie dossierstuk 91 (Beantwoording door UWV, bijlagen 1 t/m 4).
[20] Zie dossierstuk 91 (Beantwoording door UWV, bijlagen 1 t/m 4).
[21] Zie dossierstuk 86 (Beantwoording door UWV, bijlage 1 (bestand "aantallen_berichten_ap")) en dossierstuk 91 (Beantwoording door UWV, bijlage 5 (bestand "aantallen_berichten_ap")).
[22] Zie o.m. dossierstukken 8 t/m 12 en 15 t/m 21 (datalek(vervolg)meldingen bij AP) en dossierstuk 38 (Excel-bestand, antwoord op vraag 6 mbt alle datalekken).
[23] Het negende datalek is niet gemeld bij de AP, omdat UWV het niet waarschijnlijk achtte dat dit een risico voor de rechten en vrijheden van personen opleverde. Zie o.a. dossierstuk 81 (Beantwoording door UWV, bijlage 1 (bestand "Beantwoording vragen AP augustus 2019"), antwoord vraag 8)) en dossierstuk 83 (Beantwoording door UWV, antwoord vraag 8).
[24] Zie ook dossierstuk 45 (Beantwoording door UWV, bijlage "Beslisnotitie FG onderzoek", p. 2).
[25] Bron van deze gegevens: zie dossierstuk 8, 9, 10, 11, 12, 15, 16, 17, 18, 19, 20, 21, 38, 51, 81, 86 en 98.

	Datum datalek	Aantal betrokkenen waarvan de gegevens zijn gelekt	Aantal betrokkenen die het bericht hebben geopend	Soort gegevens
1	22-8-2016	195	14	Achternaam, BSN, laatste beroep, opleidingsniveau en row-ID
2	14-9-2016	151	20	Achternaam, woonplaats, geboortedatum, BSN, eerste WW-dag, datum waarop de WW afloopt en van sommigen of zij ziek of aan het werk zijn, dat ze niet per sms bereikbaar of niet digivaardig zijn
3	15-9-2016	135	26	BSN
4	22-9-2016	11062	26	Achternaam, postcode, woonplaats, e-mailadres, BSN, leeftijd, geslacht, beroep (sector), opleiding(sniveau), eerste WW-dag en datum waarop WW afloopt, of status van cv actief of verlopen is, aantal dagen WW waarop werkzoekende recht heeft, row-ID
5	21-2-2017	189	10	BSN, voorletters, achternaam, geslacht, e-mailadres, leeftijd, WERKbedrijf-locatie, eerste WW-dag, totale score op de online vragenlijst en een korte beschrijving van belemmeringen ten aanzien van het vinden van werk (zoals psychisch of lichamelijk werkvermogen), waaronder voor 73 betrokkenen gezondheidsgegevens. Deze gezondheidsgegevens betreffen geen ziektebeeld of medische rapportages, maar bijvoorbeeld wel of iemand te ziek is om te werken. Uit de eerste WW-dag kan worden afgeleid dat alle 189 betrokkenen een WW-uitkering ontvangen (niet de hoogte daarvan).
6	26-3-2018	10	7	Naam, postcode, woonplaats, opleiding(sniveau) en BSN
7	28-3-2018	90	12	Achternaam, postcode, woonplaats, beroepssector en BSN

8	3-8-2018	2503	70	Achternaam, geslacht, geboortedatum, BSN, telefoonnummer, opleidingsniveau, laatste beroep, laatste werkgever, categorieën rijbewijs, mondelinge en schriftelijke vaardigheid Nederlands, eerste, tweede en derde beroepssector, inschrijvings-/bemiddelingsberoep, beschikbare uren per week, uren nog werkzaam, eerste WW-dag, maximale laatste dag WW-uitkering, leeftijdsgroep op basis van eerste WW-dag, indicering, of er een ontheffing is en het row-ID.
9	5-9-2018	996	9	Achternaam en row-ID

2.5 Beleid binnen UWV

Binnen UWV was er vanaf in ieder geval 2016 beleid opgesteld om risico's bij de verwerking van persoonsgegevens vroegtijdig te detecteren en aan te pakken op basis van een zorgvuldige risicoafweging, waarbij risico's worden geneutraliseerd of expliciet door een directeur worden geaccepteerd. Tevens dient UWV de (uitkomsten van) risicoafwegingen op basis van het beleid te registreren.[26]

Ook was binnen UWV in ieder geval vanaf 2016 tot en met 2020 beleid opgesteld om technische en organisatorische beveiligingsmaatregelen op een risico-gestuurde wijze in te voeren en deze te controleren, evalueren en aan te passen.[27]

2.6 Praktijk binnen UWV

2.6.1 Afwegen van risico's in de praktijk

De AP heeft UWV meerdere malen gevraagd of en zo ja welke risicoanalyses zijn uitgevoerd om de persoonsgegevens bij het versturen van groepsberichten te beveiligen.[28] Hoe en welke risico's UWV precies heeft afgewogen, mede in reactie op de opgetreden datalekken, om vast te stellen of persoonsgegevens bij het versturen van groepsberichten via de Mijn Werkmap-omgeving voldoende dan wel onvoldoende beveiligd zijn heeft UWV niet vermeld.[29]

UWV blijkt in haar antwoorden geen eenduidig en zelfs soms tegenstrijdig beeld te geven over het (periodiek) uitvoeren van risicoanalyses met betrekking tot de beveiliging van persoonsgegevens bij het versturen van groepsberichten via de Mijn Werkmap-omgeving. UWV heeft in ieder geval verklaard dat zij

[26] Zie bijlage 1 pagina 25 voor de exacte delen uit de beleidsdocumenten van het UWV.
[27] Zie bijlage 1 pagina 25 voor de exacte delen uit de beleidsdocumenten van het UWV.
[28] Zie o.a. dossierstuk 27 (Brief aan UWV, p. 4-5) en dossierstuk 69 (Brief aan UWV, vraag 12) en dossierstuk 93 (E-mail aan UWV).
[29] Zie o.a. dossierstuk 38 (Excel-bestand, antwoord bij 11 onder datalek 1 t/m 4) en dossierstuk 81 (Beantwoording door UWV, bijlage 1 (bestand "Beantwoording vragen AP augustus 2019", antwoord op vraag 12)) en dossierstuk 98 (Beantwoording door UWV, bestand "Aanvullende vragen AP2110", p. 2).

geen risicoanalyse heeft uitgevoerd voorafgaand aan het besluit in 2012 om groepsberichten te gaan versturen via de Mijn Werkmap-omgeving. UWV heeft wel een aantal malen gesteld dat zij vanaf 2016 tot en met het laatste datalek in 2018 in het kader van de beveiliging van persoonsgegevens bij het versturen van groepsberichten via de Mijn Werkmap-omgeving risicoafwegingen heeft uitgevoerd. Uit de antwoorden van UWV en aangeleverde stukken is echter niet gebleken hoe deze risicoafwegingen zijn gemaakt en welke risico's daarbij op enig moment in die periode zijn afgewogen. Tevens heeft UWV de risico's niet regelmatig afgewogen.[30]

2.6.2 Maatregelen, controle en aanpassingen in de praktijk

UWV stelde in de datalekmeldingen bij de AP van het tweede en derde datalek dat zij aan het onderzoeken was of technische maatregelen mogelijk zijn om deze datalekken te voorkomen.[31] In de melding van het vierde datalek bij de AP gaf UWV aan te onderzoeken of het mogelijk was om het plaatsen van "dergelijke bestanden" in de Mijn Werkmap-omgeving te blokkeren.[32] UWV stelde in de datalekmeldingen bij de AP van het derde en het vierde datalek eind september 2016 dat de medewerker die de fout heeft gemaakt hierop door het management was aangesproken en dat er naar bewustwording werd gekeken.[33]

UWV heeft na de eerste vier datalekken in 2016 besloten tot het nemen van organisatorische maatregelen. Op 28 september 2016 heeft UWV eerst besloten tot tijdelijke organisatorische maatregelen.[34] En hoewel UWV heeft gesteld dat deze tijdelijke maatregelen ook thans nog gelden, volgt uit een besluit van het Districtsmanagers overleg (DMO) van UWV dat de tijdelijke maatregelen waartoe op 28 september 2016 was besloten, in oktober 2016 zijn vervangen door andere organisatorische maatregelen. Verder heeft de AP vastgesteld dat UWV de "Richtlijn veilig communiceren bij WERKbedrijf" heeft opgesteld en dat het voornemen om de mogelijkheden tot het nemen van technische maatregelen te onderzoeken niet door UWV is uitgevoerd. Daarnaast heeft de AP geconcludeerd dat de na 20 oktober 2016 van kracht zijnde organisatorische maatregel(en) voorafgaande aan het vijfde datalek niet is/zijn gecontroleerd noch geëvalueerd door UWV.[35]

UWV heeft vervolgens na het vijfde datalek (21 februari 2017) besloten tot nadere organisatorische maatregelen met betrekking tot het verzenden van groepsberichten via de Mijn Werkmap-omgeving, namelijk door het verhogen van de awareness daarbij. Dat deed UWV door workshops en enkele bezoeken aan districten. UWV heeft toen besloten geen technische maatregelen te nemen. Overigens zijn de na 20 oktober 2016 van kracht zijnde organisatorische maatregel(en) met betrekking tot het verzenden van groepsberichten via de Mijn Werkmap-omgeving ook niet voorafgaande aan het zesde datalek door UWV gecontroleerd noch geëvalueerd.[36] De stelling van UWV dat deze maatregelen wel heeft gecontroleerd en geëvalueerd, heeft UWV niet onderbouwd met documentatie.

[30] Zie bijlage 1 pagina 26 en 27 voor de exacte antwoorden van het UWV.
[31] Zie dossierstukken 9 en 10 (Datalekmeldingen).
[32] Zie dossierstukken 11 en 12 (Datalek(vervolg)meldingen).
[33] Zie dossierstuk 10 (Datalekmelding) en dossierstukken 11 en 12 (Datalek(vervolg)meldingen).
[34] Zie bijlage 1 pagina 28 en 29 voor de exacte maatregelen van het UWV.
[35] Zie bijlage 1 pagina 30 t/m 34 voor de exacte maatregelen en verklaringen van het UWV.
[36] Zie bijlage 1 pagina 33 t/m 35 voor de exacte maatregelen en verklaringen van het UWV.

Na het zevende datalek (28 maart 2018) heeft UWV tot meerdere organisatorische maatregelen besloten. UWV en het WERKbedrijf hebben echter niet als zodanig gecontroleerd of deze maatregelen daadwerkelijk zijn ingevoerd.[37] Buiten twee maatregelen[38] heeft UWV ook geen documenten of een nadere onderbouwing aangeleverd op basis waarvan kan worden vastgesteld of de organisatorische maatregelen zijn geborgd in documentatie en wanneer deze zijn geïmplementeerd.

UWV heeft na het achtste datalek (3 augustus 2018) besloten tot het invoeren van een technische maatregel, namelijk het blokkeren van de mogelijkheid tot het toevoegen van onder andere Excel-bestanden bij het verzenden van groepsberichten via de Mijn Werkmap-omgeving om datalekken daarbij te voorkomen. Deze technische maatregel is in december 2018, dus ver na het negende datalek, door UWV ingevoerd.
De bovengenoemde feiten gaan over de periode van 2012 tot en met 2018. Dit besluit en het onderzoek van de AP hebben alleen betrekking op deze periode. UWV heeft in haar zienswijze wel nog het volgende verklaard over de periode na 2018.

UWV heeft verklaard dat in het proces voor het versturen van groepsberichten in de Mijn Werkmap-omgeving naast de technische maatregel, die het specifieke risico op het versturen van Excel-lijsten heeft weggenomen, ook actief is ingezet op extra bewustwording bij (nieuwe) medewerkers in de uitvoering die voor de uitvoering van hun taken veelvuldig (digitaal) contact hebben met werkzoekenden. Daarnaast worden nu binnen WERKbedrijf de procesbeschrijvingen en Quick Reference Cards (QRC's) jaarlijks geëvalueerd en indien nodig aangepast.

Verder heeft de FG eind 2018 in opdracht van de Raad van Bestuur van UWV een onderzoek uitgevoerd naar aanleiding van het achtste datalek en een rapportage van bevindingen opgesteld. Specifiek voor het mitigeren van de risico's bij het verzenden van groepsberichten in de Mijn Werkmap-omgeving, stelt het FG-onderzoek dat de technische maatregel die Excel-bestanden uploaden naar de Mijn Werkmap-omgeving onmogelijk maakt, een effectieve maatregel is om dit type datalekken te voorkomen.

Mede naar aanleiding van het FG-onderzoek heeft UWV WERKbedrijf verder aan KPMG de opdracht gegeven om een breder onderzoek uit te voeren naar het bronsysteem SONAR. Dit om te bepalen waar de kwetsbaarheden en risico's zich bevinden op technisch, procesmatig als ook organisatorisch gebied, waarbij tevens de reeds bestaande organisatorische en technische maatregelen zijn geëvalueerd (check-fase). Dit onderzoek heeft in 2020 geresulteerd in vier adviesrapporten met 77 aanbevelingen. Het adviesrapport privacy is grotendeels door UWV openbaar gemaakt.[39]

Naar aanleiding van de adviesrapporten is in 2020 het grootschalige verbeterproject SONAR IB&P gestart, dat tot doel heeft de bevindingen uit het onderzoek te adresseren en het IB&P-risiconiveau van SONAR sterk te reduceren (act->plan->do-fasen). In dat kader zal UWV een extra technische maatregel

[37] Zie bijlage 1 pagina 35 t/m 41 voor de exacte maatregelen en verklaringen van het UWV.
[38] Het 'Stappenplan Veilig Persoonsgegevens delen' wat UWV op 1 mei 2018 heeft gecommuniceerd aan medewerkers. Tevens had UWV de QRC groepsberichten uitgebreid met de passage over het schonen van (Excel-)bestanden en het 4-ogenprincipe.
[39] Zie https://www.uwv.nl/overuwv/Images/bijlage-1-bij-besluit-wob-verzoek-onderzoeksrapport-sonar-privacy.pdf.

doorvoeren. De exportfunctionaliteit uit SONAR voor medewerkers in de uitvoering, behoudens enkele geautoriseerde medewerkers, zal namelijk dichtgezet worden.

De aanbevelingen uit het KPMG onderzoek zien volgens UWV ook toe op het verbeteren van het risicomanagementproces, waaronder ook de Plan-Do-Check-Act-cyclus (hierna: PDCA-cyclus). Met deze verbetering in het risicomanagement en het implementeren van beheersingsmaatregelen zal het WERKbedrijf de groei in het invulling geven aan de PDCA-cyclus – en daarmee waarborgen dat er passende technische en organisatorische maatregelen getroffen zijn en worden – verder doorzetten.

3. Juridische beoordeling

3.1 Verwerking van persoonsgegevens

Per 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing.[40] Gezien de feiten in dit onderzoek plaats vonden tussen 2012 en 2018, zal de AP zowel aan de Wet bescherming persoonsgegevens (Wbp) als de AVG toetsen.

Het begrip persoonsgegeven is gedefinieerd in artikel 1, onder a, van de Wbp en artikel 4, onderdeel 1, van de AVG. In artikel 16 van de Wbp worden persoonsgegevens over de gezondheid als bijzondere persoonsgegevens aangemerkt. De AVG merkt in artikel 9 gegevens over gezondheid eveneens als bijzondere persoonsgegevens aan.

Persoonsgegevens in de zin van de Wbp en de AVG zijn alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. In Sonar zijn gegevens over natuurlijke personen opgenomen zoals namen, adressen, het BSN en andere gegevens. Middels deze gegevens kunnen de in Sonar geregistreerde natuurlijke personen, waaronder werkzoekenden, direct of indirect worden geïdentificeerd. Sonar bevat dus persoonsgegevens in de zin van artikel 1, onder a, van de Wbp en artikel 4, onderdeel 1, van de AVG.

In Sonar zijn ook gegevens opgenomen over fysieke beperkingen en het psychisch en lichamelijk werkvermogen van personen. Tevens staat in Sonar of personen zich te ziek voelen om te werken. Op grond van artikel 16 van de Wbp en artikel 4, onderdeel 15, van de AVG zijn dit gegevens over de gezondheid.

Uit bovenstaande volgt dat UWV bij het verzenden van groepsberichten via de Mijn Werkmap-omgeving persoonsgegevens, waaronder het BSN en gegevens over de gezondheid, verwerkt in de zin van de Wbp en de AVG.

[40] Op die datum is ingevolge artikel 51 van de UAVG de Wet bescherming persoonsgegevens (Wbp) ingetrokken.

3.2 Verwerkingsverantwoordelijke

Het begrip (verwerkings)verantwoordelijke wordt gedefinieerd in artikel 1, onder d, van de Wbp en artikel 4, onderdeel 7, van de AVG. Bij zelfstandige bestuursorganen op rijksniveau zal het orgaan, belast met de taken en uitoefening van bevoegdheden waarvoor de gegevens worden verwerkt, als verantwoordelijke zijn aan te merken.

Zoals vermeld in paragraaf 2.1 is UWV ingesteld op grond van een wet, namelijk de SUWI. UWV is een zelfstandig bestuursorgaan van de Rijksoverheid met eigen rechtspersoonlijkheid. Zoals hierboven vermeld is bij zelfstandige bestuursorganen op rijksniveau het orgaan, belast met de taken en uitoefening van bevoegdheden waarvoor de gegevens worden verwerkt, als verantwoordelijke aan te merken. UWV heeft zowel de juridische als de feitelijke zeggenschap over de verwerking van persoonsgegevens die worden verzameld in het kader van het verzenden van groepsberichten via de werkmap.

Op grond van het bovenstaande merkt de AP UWV aan als (verwerkings)verantwoordelijke als bedoeld in artikel 1, onder d, van de Wbp en artikel 4, onderdeel 7, van de AVG voor de verwerking van persoonsgegevens in het kader van het verzenden van groepsberichten via de werkmap.

3.3 Beveiliging van de verwerking van persoonsgegevens

3.3.1 Juridisch kader

Van 1 september 2001 tot 25 mei 2018 gold ten aanzien van de beveiliging van de verwerking van persoonsgegevens artikel 13 van de Wbp. De beveiligingsverplichting strekt zich uit tot alle onderdelen van het proces van gegevensverwerking. In het begrip «passende» ligt besloten dat de beveiliging in overeenstemming is met de stand van de techniek. Dit is in eerste aanleg een vraag van professionele ethiek van personen belast met de informatiebeveiliging. De normen van deze ethiek worden in deze bepaling van een juridisch sluitstuk voorzien, in die zin dat daaraan een wettelijke verplichting voor de verantwoordelijke is verbonden. Het begrip «passend» duidt mede op een proportionaliteit tussen de beveiligingsmaatregelen en de aard van de te beschermen gegevens. Naarmate bijvoorbeeld de 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 de gegevens.

De Europese richtlijn op grond waarvan onder meer artikel 13 van de Wbp is opgesteld overweegt onder andere het volgende ten aanzien van de beveiliging van de verwerking van persoonsgegevens: "*dat de beginselen van de bescherming (...) tot uiting moeten komen in de verplichtingen die aan de personen, overheidsinstanties, ondernemingen of andere lichamen die de verwerkingen uitvoeren , worden opgelegd, verplichtingen die met name betrekking hebben op de kwaliteit van de gegevens , de technische beveiliging, de aanmelding bij de toezichthoudende autoriteit en de omstandigheden waarin de verwerking kan worden uitgevoerd (...)*".[41] Tevens wordt hierin ten aanzien van de beveiliging van de verwerking van persoonsgegevens overwogen: "*dat de bescherming van de rechten en vrijheden van de betrokkenen in verband met de verwerking van persoonsgegevens zowel bij het ontwerpen als*

[41] Zie Richtlijn 95/46/EG van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, overweging 25. Onderstreping van de AP.

bij de uitvoering van de verwerking passende technische maatregelen vergt, in het bijzonder om de veiligheid te waarborgen en zodoende elke ongeoorloofde verwerking te verhinderen; (...)".[42]

Het CBP heeft - in een zaak waarbij het ging om toegang tot elektronische medische dossiers - ten aanzien van het treffen van beveiligingsmaatregelen in het kader van artikel 13 van de Wbp als volgt geoordeeld: "*Een verantwoordelijke mag pas overgaan tot het treffen van louter organisatorische maatregelen als hij kan aantonen dat het niet mogelijk is passende technische maatregelen te nemen. Dit dient dan wel gecompenseerd te worden met extra organisatorische maatregelen en controle op de naleving hiervan*".[43]

Ter invulling van artikel 13 van de Wbp heeft het CBP in 2013 richtsnoeren ten aanzien van de beveiliging van de verwerking van persoonsgegevens (hierna: CBP-richtsnoeren) opgesteld.[44] Bij het opstellen van de CBP-richtsnoeren is aansluiting gezocht bij de ISO27001. De richtsnoeren stellen als noodzakelijke randvoorwaarden om tot een continue passend beveiligingsniveau van de verwerking van persoonsgegevens te komen en te garanderen zoals de wet voorschrijft: "*maatregelen treffen op basis van risicoanalyse, beveiligingsstandaarden toepassen en de inbedding in een plan-do-check-act-cyclus*".

Over deze PDCA-cyclus staat in de CBP-richtsnoeren: ''*Na het vaststellen van de betrouwbaarheidseisen treft de verantwoordelijke maatregelen waarmee hij waarborgt dat aan de betrouwbaarheidseisen wordt voldaan. Vervolgens controleert de verantwoordelijke of de maatregelen daadwerkelijk getroffen zijn en het gewenste effect sorteren. Het totaal aan betrouwbaarheidseisen, maatregelen en controle wordt regelmatig geëvalueerd en waar nodig aangepast, waardoor een blijvend passend beveiligingsniveau wordt bereikt*".[45]

Net als ISO27001 schrijven ook de CBP-richtsnoeren (als onderdeel van de PDCA-cyclus) voor dat de verwerkingsverantwoordelijke beveiligingsmaatregelen treft op basis van een risicoanalyse, waarbij hij de dreigingen inventariseert die kunnen leiden tot een beveiligingsincident, de gevolgen die het beveiligingsincident kan hebben en de kans dat deze gevolgen zich voordoen. Bij het inventariseren en beoordelen van de risico's zijn vooral de gevolgen relevant die betrokkenen kunnen ondervinden van onrechtmatige verwerking van hun persoonsgegevens. Deze gevolgen kunnen, afhankelijk van de aard van de verwerking en van de verwerkte persoonsgegevens, onder meer bestaan uit stigmatisering of uitsluiting, schade aan de gezondheid of blootstelling aan (identiteits)fraude.[46]

In de AVG zijn in artikel 32 de eisen rondom de beveiliging van de verwerking van persoonsgegevens opgenomen. Bij het bepalen van passende maatregelen dient rekening gehouden te worden met het risico voor de rechten en vrijheden van personen.[47]

Overweging 83 van de AVG stelt ten aanzien van het waarborgen van de beveiliging van de verwerking van persoonsgegevens en de beoordeling van de risico's: "*Teneinde de veiligheid te waarborgen en te voorkomen dat de*

[42] Zie Richtlijn 95/46/EG, overweging 46. Onderstreping van de AP.
[43] Zie o.a. zaak Z2003-0145, p. 3.
[44] Zie CBP richtsnoeren: beveiliging van persoonsgegevens, https://wetten.overheid.nl/BWBR0033572/2013-03-01.
[45] Zie CBP richtsnoeren: beveiliging van persoonsgegevens, https://wetten.overheid.nl/BWBR0033572/2013-03-01.
[46] Zie CBP richtsnoeren: beveiliging van persoonsgegevens, https://wetten.overheid.nl/BWBR0033572/2013-03-01.
[47] Zie ook overweging 75 van de AVG.

verwerking inbreuk maakt op deze verordening, dient de verwerkingsverantwoordelijke of de verwerker de aan de verwerking inherente risico's te beoordelen en maatregelen, zoals versleuteling, te treffen om die risico's te beperken. Die maatregelen dienen een passend niveau van beveiliging, met inbegrip van vertrouwelijkheid, te waarborgen, rekening houdend met de stand van de techniek en de uitvoeringskosten afgezet tegen de risico's en de aard van de te beschermen persoonsgegevens. Bij de beoordeling van de gegevensbeveiligingsrisico's dient aandacht te worden besteed aan risico's die zich voordoen bij persoonsgegevensverwerking, zoals de vernietiging, het verlies, de wijziging, de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot de doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig, hetgeen met name tot lichamelijke, materiële of immateriële schade kan leiden."

Tot slot is in 2007 het Besluit voorschrift informatiebeveiliging rijksdienst (hierna: VIR) van kracht geworden.[48] In de Bestuurlijke verklaring Informatieveiligheid uit 2014 verklaart UWV het VIR te gaan hanteren.[49] Ten aanzien van in het VIR gebruikte begrippen wordt aangegeven: "*Het begrippenkader van de Code van Informatiebeveiliging (ISO17799:2005) is in dit voorschrift overgenomen*".[50] De PDCA-cyclus uit ISO17799:2005 is inmiddels opgenomen in ISO27001.[51] Deze standaard bevat een aantal stappen die uitgevoerd dienen te worden. De stappen vormen een zogenaamde Plan-Do-Check-Act-cyclus (hierna: PDCA-cyclus) om in te spelen op (steeds wisselende) bedreigingen ten aanzien van de informatie.[52]

In artikel 4 VIR worden de verantwoordelijkheden van het lijnmanagement aangeduid. In de algemene toelichting bij het VIR is over artikel 4 VIR het volgende opgenomen: "*Er is bewust gekozen om artikel 4 in termen van de Planning en Control cyclus, conform reguliere bedrijfsvoering, te formuleren. (...) Informatiebeveiliging zelf vindt plaats via de kwaliteitscirkel van Deming (PDCA cyclus)*".[53] In de artikelsgewijze toelichting bij het VIR staat daarnaast ten aanzien van artikel 4: "*Voor het effectueren van informatiebeveiliging wordt gewerkt via de Plan Do Check Act cyclus (...). Na het vaststellen wat nodig is (betrouw-baarheidseisen), worden maatregelen getroffen en gecontroleerd of die maatregelen het gewenste effect sorteren (controle). Deze controle kan direct aanleiding geven tot bijsturing in de maatregelen. Ook kan het totaal van eisen, maatregelen en controle aan revisie toe zijn (evaluatie). Het goed doorlopen van deze kwaliteitscirkel zorgt op elk moment voor het adequate beveiligingsniveau*".[54]

3.3.2 Beoordeling

Uit zowel artikel 13 van de Wbp als artikel 32, eerste en tweede lid, van de AVG vloeit voort dat de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen moet nemen om een op het risico afgestemd beveiligingsniveau van de verwerking van persoonsgegevens te garanderen/waarborgen. Deze bepalingen beogen dezelfde (rechts)belangen te waarborgen en er is geen (wezenlijke) materiële wijziging van de regelgeving op dit punt.

Om een op het risico afgestemd beveiligingsniveau van de verwerking van persoonsgegevens te garanderen/waarborgen, dient een verwerkingsverantwoordelijke aldus risico's te analyseren, passende

[48] Staatscourant 28 juni 2007, nr. 122. https://zoek.officielebekendmakingen.nl/stcrt-2007-122-p11-SC81084.html.
[49] Staatscourant 2014, 15447, https://zoek.officielebekendmakingen.nl/stcrt-2014-15447.html.
[50] Staatscourant 28 juni 2007, nr. 122, p. 12.
[51] ISO/IEC 27001:2013 hoofstukken 6 t/m 10.
[52] Zie o.a. ISO/IEC 27001:2013, hoofstukken 6 t/m 10 en ISO/IEC 27001:2017.
[53] Staatscourant 28 juni 2007, nr. 122, p. 12.
[54] Staatscourant 28 juni 2007, nr. 122, p. 15-16.

maatregelen te nemen en deze te evalueren. Deze stappen vormen de randvoorwaarden om een continue passend beveiligingsniveau van de verwerking van persoonsgegevens te garanderen in lijn met de wet, namelijk door de inbedding in een plan-do-check-act-cyclus (PDCA-cyclus). Deze cyclus is in lijn met de procedure genoemd in artikel 32, eerste lid onder d, van de AVG, te weten een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking. Ook het VIR, waar het UWV zich aan heeft geconformeerd, is gebaseerd op ISO27001 en schrijft een PDCA-cyclus voor. Deze algemeen geaccepteerde beveiligingsstandaard neemt de AP in dit geval mede in ogenschouw. De AP werkt de verschillende stappen van de PDCA-cyclus hierna verder uit.

Het afwegen van risico's voor personen voorafgaande aan bepalen van maatregelen
Het startpunt dat wordt uitgevoerd in het kader van het beveiligen van de verwerking van persoonsgegevens is een afweging van de risico's van die verwerking. Op basis daarvan wordt bepaald welke maatregelen nodig zijn om deze risico's tegen te gaan.

Uit de Wbp en de AVG en de uitleg daarvan volgt dat bij de afweging van de gegevensbeveiligingsrisico's aandacht dient te worden besteed aan risico's die zich voordoen bij persoonsgegevensverwerking. Zoals ongeoorloofde verstrekking van of ongeoorloofde toegang tot verwerkte gegevens. Bij het inventariseren en beoordelen van de risico's zijn vooral de *gevolgen* relevant die personen kunnen ondervinden van een onrechtmatige verwerking van persoonsgegevens. Naarmate de 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 de persoonsgegevens.

Bij het verzenden van groepsberichten via de Mijn Werkmap-omgeving is, zoals vermeld in paragraaf 2.4, herhaaldelijk sprake geweest van een (per ongeluk) ongeoorloofde verstrekking dan wel ongeoorloofde toegang van verwerkte persoonsgegevens van werkzoekenden. Van UWV wordt dan ook verwacht dat zij, om tot een op de risico's afgestemd beveiligingsniveau te komen, continu de risico's inventariseert en beoordeelt die kunnen leiden tot een beveiligingsincident. Binnen UWV bestond vanaf in ieder geval 2016 beleid om risico's bij de verwerking van persoonsgegevens vroegtijdig te detecteren en aan te pakken op basis van een zorgvuldige risicoafweging. Ook het VIR verplicht UWV tot een expliciete risicoafweging bij het bepalen van passende beveiligingsmaatregelen.

Zoals in paragraaf 3.1 de AP heeft geconcludeerd, verwerkt UWV in Sonar een veelheid aan verschillende persoonsgegevens met een zeer gevoelig karakter, waaronder gegevens over de gezondheid van personen en het BSN. UWV verwerkte in de periode van 2016 tot en met 2018 gegevens over gemiddeld 4.500.000 personen. Werkzoekenden, zieken en arbeidsongeschikten die wettelijk verplicht zijn zich te registreren bij UWV en daarvoor hun persoonsgegevens moeten verstrekken, moeten erop kunnen vertrouwen dat UWV op een deugdelijke wijze de risico's afweegt die deze personen lopen. De gevolgen van een beveiligingsincident met betrekking tot de persoonsgegevens die UWV verwerkt kunnen ernstig zijn voor een grote groep personen. Zo kan het onvoldoende beveiligen van de verwerking van deze persoonsgegevens leiden tot stigmatisering of uitsluiting. Nu UWV ook het BSN verwerkt wat in de

praktijk een koppeling van verschillende bestanden aanzienlijk vergemakkelijkt, bestaat er voor personen wiens gegevens in Sonar staan een extra risico op bedreiging van de persoonlijke levenssfeer.

Het beleid van UWV bevat maatregelen, waaronder een expliciete risicoafweging als onderdeel van een PDCA-cyclus. In tegenstelling tot dit beleid blijkt dat UWV in hun beantwoording ten aanzien van het versturen van groepsberichten via de Mijn Werkmap-omgeving een tegenstrijdig beeld geeft over het uitvoeren van dergelijke risicoanalyses met betrekking tot de beveiliging van persoonsgegevens. UWV heeft in ieder geval verklaard dat voorafgaande aan het besluit in 2012 om alleen nog groepsberichten te versturen via de Mijn Werkmap-omgeving geen risicoanalyse is uitgevoerd. Vervolgens heeft UWV gesteld dat zij vanaf 2016 tot en met het laatste datalek in 2018 in het kader van de beveiliging van persoonsgegevens bij het versturen van groepsberichten via de Mijn Werkmap-omgeving risicoafwegingen heeft uitgevoerd. Uit de antwoorden van UWV en aangeleverde stukken is echter niet gebleken hoe UWV deze risicoafwegingen heeft gemaakt en welke risico's daarbij op enig moment in die periode zijn afgewogen en hoe daarbij is stilgestaan met de mogelijke gevolgen voor werkzoekenden. Voor zover UWV van mening is dat de voorgestelde maatregelen van oktober 2016[55] wel een risicoafweging bevat, merkt de AP op dat hierin geen afweging van risico's in de zin van de (uitleg van de) wet is waar te nemen. Het bevat slechts een voorstel voor maatregelen zonder verdere onderbouwing. Tevens blijkt uit dit document niet dat risico's voor personen zijn meegewogen bij het voorstellen van maatregelen. Sterker nog, UWV spreekt slechts over risico's die UWV zelf loopt in haar klantcommunicatie. Juist bij een organisatie als UWV, die zoveel bijzondere en gevoelige persoonsgegevens van zoveel personen verwerkt, en de gevolgen voor hen bij het verzenden van groepsberichten via de Mijn werkmap-omgeving verstrekkend kunnen zijn, is het niet of onvoldoende rekening houden met de risico's voor werkzoekenden bij het vaststellen van beveiligingsmaatregelen extra onzorgvuldig.

Op grond van het bovenstaande concludeert de AP dat UWV ten aanzien van het treffen van beveiligingsmaatregelen in het kader van het verzenden van groepsberichten via de Mijn Werkmap-omgeving de risico's voor werkzoekenden, die gezien de gevoeligheid van de gegevens die UWV verwerkt ingrijpend kunnen zijn, in ieder geval in de periode van 2012 tot en met 2018 niet/onvoldoende in kaart heeft gebracht. Hiermee heeft UWV onvoldoende een op risico afgestemd beveiligingsniveau gegarandeerd en gewaarborgd.

Treffen van technische en organisatorische maatregelen

Na het in kaart brengen en wegen van de risico's voor personen van de verwerking van persoonsgegevens dienen de vastgestelde maatregelen vervolgens geïmplementeerd en uitgevoerd te worden. Zowel artikel 13 van de Wbp als artikel 32, eerste lid, van de AVG verplichten de verwerkingsverantwoordelijke tot het nemen van technische en organisatorische maatregelen om de beveiliging van de verwerking van persoonsgegevens te waarborgen.

Uit paragraaf 2.6 blijkt dat UWV tot december 2018 slechts organisatorische maatregelen heeft doorgevoerd in het kader van het verzenden van groepsberichten via de Mijn Werkmap-omgeving om de beveiliging van de verwerking van persoonsgegevens te waarborgen. Een voorbeeld van een

[55] Zie bijlage 1 pagina 30.

organisatorische maatregel is het bericht waar medewerkers worden opgeroepen bij voorkeur geen bijlagen mee te zenden met groepsberichten via Sonar. De maatregel ten aanzien van een beperking op het aantal werkzoekenden aan wie het bericht kan worden verzonden diende verder, zoals UWV ook zelf stelt, om technische problemen in Sonar te voorkomen waardoor de werking en stabiliteit daarvan verbetert en het berichtenverkeer soepeler verloopt. Dit dient dus niet om de beveiliging van de verwerking van persoonsgegevens te waarborgen. Deze beperking ziet slechts op het aantal ontvangers van een bericht, maar beperkt niet het aantal werkzoekenden wiens persoonsgegevens door UVW kunnen worden verstuurd. Bovendien kon de beperking tot 100 geadresseerden omzeild worden door een verzoek daartoe te doen bij Functioneel Beheer. Bij vijf van de negen datalekken is hetzelfde groepsbericht aan meer dan 100 werkzoekenden tegelijk verstuurd via de Mijn Werkmap-omgeving.

UWV had op 20 oktober 2016 (na het vierde datalek) besloten om op korte termijn een onderzoek te starten naar de mogelijkheid tot het nemen van technische maatregelen, waaronder het technisch onmogelijk maken om Excel-bestanden aan een werkmapbericht toe te voegen. Het heeft dan nog tot na het achtste datalek in september 2018 geduurd voordat UWV vervolgens heeft besloten tot het nemen van een technische maatregel, namelijk het blokkeren van de mogelijkheid tot het toevoegen van onder andere Excel-bestanden bij het verzenden van groepsberichten via de Mijn werkmap-omgeving. Echter blijkt dat UWV pas in december 2018 (ver na het negende datalek op 5 september 2018 en ver na het in 2016 aangekondigde onderzoek naar het invoeren van technische maatregelen) is overgegaan om het drie maanden eerder genomen besluit ook daadwerkelijk uit te voeren. Het nemen van deze technische maatregel was derhalve mogelijk.

De datalekken vormden kennelijk voor UWV geen urgente aanleiding om het in 2016 geopperde onderzoek naar de mogelijkheid van technische maatregelen alsnog spoedig uit te voeren. Door het niet (tevens) doorvoeren van een technische maatregel heeft UWV onvoldoende een op risico afgestemd beveiligingsniveau gewaarborgd en daarmee meer dan twee jaar een risico geaccepteerd van datalekken met veel persoonsgegevens betreffende een grote groep burgers.

Controleren en aanpassen van maatregelen

Technische en organisatorische beveiligingsmaatregelen dienen zowel op basis van de Wbp als de AVG een op het risico afgestemd beveiligingsniveau te waarborgen. Hiervoor is het in ieder geval noodzakelijk om te controleren of de maatregelen zijn geïmplementeerd, juist worden toegepast of uitgevoerd en wat het effect van de maatregelen is op de initieel geïdentificeerde risico's. Op basis van deze controle van de maatregelen stelt men vervolgens vast of de maatregelen nog steeds een op het risico afgestemd beveiligingsniveau waarborgen dan wel of additionele maatregelen nodig zijn.

Binnen UWV geldt vanaf in ieder geval 2016 tot en met 2020 beleid om getroffen maatregelen te controleren en zo nodig aan te passen als onderdeel van een PDCA-cyclus. UWV meldt hierover echter dat UWV geen generiek beleid heeft waarin het controleert of UWV-centrale maatregelen zijn geïmplementeerd in de praktijk door de verantwoordelijke divisie(s) en dat regiokantoren tot op zekere hoogte een eigen invulling kunnen geven aan centraal beleid. Tevens meldt UWV hierover dat er geen formeel geprotocolleerde procedure is binnen UWV waarbinnen er op centraal niveau wordt

gecontroleerd of dergelijke afgesproken organisatorische- en procesmatige maatregelen worden uitgevoerd, omdat dat ondoenlijk zou zijn gezien de omvang van de organisatie en de hoeveelheid beslissingen die UWV neemt.

Ook geeft UWV aan dat zij niet heeft gecontroleerd of maatregelen waartoe was besloten naar aanleiding van datalekken wel daadwerkelijk zijn ingevoerd. UWV heeft daarnaast de na 20 oktober 2016 van kracht zijnde organisatorische maatregel(en) voorafgaande aan het vijfde (2017) en zesde (2018) datalek niet gecontroleerd noch geëvalueerd. Tot slot heeft UWV niet aangetoond dat zij op enig moment heeft gecontroleerd of de organisatorische maatregelen die golden voorafgaande aan het achtste datalek (2018) zijn ingevoerd. Ook heeft UWV deze organisatorische maatregelen niet geëvalueerd.

Zoals eerder geconcludeerd zijn de gevolgen voor werkzoekenden bij het onvoldoende beveiligd verzenden van groepsberichten via de werkmap verstrekkend. Juist bij een organisatie als UWV, die zoveel gevoelige en bijzondere persoonsgegevens van zoveel personen verwerkt, is het noodzakelijk om te controleren of maatregelen daadwerkelijk (correct) zijn geïmplementeerd en deze te evalueren en waar nodig aan te passen. Werkzoekenden en anderen die wettelijk verplicht zijn zich te registreren bij UWV en daarvoor hun persoonsgegevens moeten verstrekken, moeten erop kunnen vertrouwen dat UWV maatregelen controleert, evalueert en zo nodig aanpast.

Op grond van het bovenstaande concludeert de AP dat UWV de getroffen beveiligingsmaatregelen in het kader van het verzenden van groepsberichten via de Mijn Werkmap-omgeving niet/onvoldoende heeft gecontroleerd en geëvalueerd, waardoor UWV onvoldoende een op risico afgestemd beveiligingsniveau heeft gegarandeerd en gewaarborgd.

3.4 Zienswijze UWV en reactie AP

De AP geeft in deze paragraaf de zienswijze van UWV kort weer met daarop de reactie van de AP.

UWV merkt allereerst op dat zij het betreurt dat er op onvoldoende wijze invulling is gegeven aan de verschillende fasen van de PDCA-cyclus. UWV trekt de bevindingen van de AP zeer aan en zet er stevig op in om dit proces te verbeteren.

3.4.1 Zienswijze op feitelijke bevindingen

UWV is van mening dat uit de analyse van het achtste datalek wel blijkt dat het achtste datalek en de direct getroffen maatregelen zowel geanalyseerd als geëvalueerd zijn door UWV, waarbij ook maatregelen worden voorgesteld.

De AP merkt hierover op dat UWV het achtste datalek inderdaad heeft geanalyseerd en geëvalueerd, maar uit deze analyse blijkt niet dat UWV de verwerking van persoonsgegevens in het kader van het verzenden van groepsberichten via de Mijn Werkmap-omgeving op zichzelf heeft geëvalueerd. De evaluatie van een los datalek is onvoldoende invulling van een op risico afgestemd beveiligingsniveau met bijbehorend PDCA-cyclus. Uit de analyse is daarnaast niet af te leiden dat UWV direct een maatregel heeft getroffen. Over het invoeren van de technische maatregel is wel door UWV gesproken, maar deze maatregel is pas

later ingevoerd. Daarnaast acht de AP hier het evalueren van maatregelen die net zouden zijn ingevoerd niet zinvol.

UWV leest niet terug in de bevindingen dat zij in augustus 2019 heeft aangegeven dat het WERKbedrijf een extern onderzoek zou laten uitvoeren naar de exportfunctionaliteit vanuit Sonar en naar het verzenden van groepsberichten via de werkmap.

De AP heeft het plan van UWV om een extern onderzoek te laten uitvoeren niet opgenomen als een feit omdat dit slechts nog een voornemen was van UWV. Daarnaast ziet dit voornemen niet op de periode van de vastgestelde overtreding. Wel heeft de AP dit onderzoek vermeld in paragraaf 2.6 van onderhavig besluit.

3.4.2 Zienswijze op juridisch kader en de beoordeling

De norm dat een verantwoordelijke pas mag overgaan tot het treffen van louter organisatorische maatregelen als hij kan aantonen dat het niet mogelijk is passende technische maatregelen te nemen, volgt volgens UWV onvoldoende uit de CBP-richtsnoeren over beveiliging uit 2013, een CBP zaak[56] en de overige bronnen die in het rapport aangehaald worden.

De AP volgt deze zienswijze van UWV niet. Ten eerste heeft de AP niet alleen verwezen naar een CBP zaak, maar ook naar de Richtlijn 95/46/EG van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, overweging 25 en 46. Ten tweede staat zowel in artikel 13 van de Wbp als artikel 32 van de AVG dat de verwerkingsverantwoordelijke passende technische *en* organisatorische maatregelen moet nemen. Technische en organisatorische maatregelen dienen cumulatief te worden getroffen. De norm in artikel 13 van de Wbp en artikel 32 van de AVG is aldus volgens de AP afdoende duidelijk. UWV heeft verder ook niet aangevoerd dat zij zich tot het treffen van uitsluitend organisatorische maatregelen mocht beperken, aangezien het niet mogelijk was om passende technische maatregelen te nemen. Een dergelijk standpunt zou overigens ook onhoudbaar zijn geweest, nu UWV in december 2018 juist uiteindelijk een technische maatregel heeft geïmplementeerd.

Dat niet alle maatregelen even effectief waren en er hierbij mogelijk verkeerde beoordelingen zijn gemaakt, kan in optiek van UWV niet de conclusie getrokken worden dat geen of onvoldoende invulling is gegeven aan het doorvoeren van passende maatregelen. En uit het enkele gegeven dat er enige tijd heeft gezeten tussen het evaluatiemoment en het invoeren van de technische maatregel kan volgens UWV, op basis van de bevindingen, niet geconcludeerd worden dat er vanaf het achtste datalek geen of onvoldoende invulling is gegeven aan het doorvoeren van passende maatregelen, als gevolg van onvoldoende risicomanagement.

De AP volgt deze zienswijze van UWV niet en motiveert dit als volgt. De AP heeft in het geheel beoordeeld of UWV voor de desbetreffende verwerking een op het risico afgestemd beveiligingsniveau heeft gegarandeerd en gewaarborgd. Dat UWV enkele organisatorische maatregelen heeft genomen doet niet af aan de vaststelling dat UWV risicoanalyses, technische maatregelen en controles onvoldoende heeft uitgevoerd. Dit heeft tot gevolg, zoals UWV ook zelf stelt, dat de beveiligingsmaatregelen niet effectief

[56] https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/arbodienst-handelt-niet-strijd-met-wbp-%C2%A0

waren. Daarnaast kwam UWV pas na het achtste datalek (3 augustus 2018) met de aanbeveling om een technische maatregel te nemen, terwijl in oktober 2016 in het Districtsmanager overleg al besloten was dat op korte termijn de mogelijkheid van technische mogelijkheden moest worden onderzocht. In deze tussenliggende periode van bijna 2 jaar heeft UWV aldus nagelaten om dit onderzoek uit te voeren.

UWV is verder van mening dat er na het achtste datalek wel een evaluatie heeft plaatsgevonden. Op basis van zienswijze hierboven volgt UWV daarom de duur van de geconstateerde overtreding niet. Volgens UWV heeft men na het achtste datalek wel een passend beveiligingsniveau gehanteerd.

De AP is het met UWV eens dat het achtste datalek is geëvalueerd. Deze evaluatie behelst echter alleen één datalek. De AP wil graag nogmaals benadrukken dat UWV de getroffen maatregelen niet periodiek in zijn geheel heeft geëvalueerd en ook niet van tevoren de risico's voldoende heeft geanalyseerd. Het FG onderzoek vond bovendien pas plaats vanaf november 2018 en de technische maatregel is door UWV in december 2018 ingevoerd. De AP volgt daarom ook niet de zienswijze dat UWV vanaf het achtste datalek (3 augustus 2018) een op risico afgestemd beveiligingsniveau heeft gegarandeerd en gewaarborgd.

Achteraf bezien, met de kennis van nu, is het proces volgens UWV niet in voldoende mate gevolgd en is er onvoldoende gedocumenteerd. UWV merkt hierbij wel op dat uit de bevindingen niet blijkt dat er in zijn geheel geen invulling is gegeven aan de verschillende fasen van de PDCA-cyclus dan wel in de gehele periode van 2012 tot en met eind 2018.

De AP beaamt dat uit de bevindingen niet blijkt dat er in zijn geheel geen invulling is gegeven aan de verschillende fasen van de PDCA-cyclus, maar stelt wel vast dat hier *onvoldoende* invulling aan is gegeven. In hetgeen UWV wel heeft gedocumenteerd blijkt dat er alleen rekening werd gehouden met het vastlopen van de systemen van UWV waarbij de risico's voor betrokkenen niet werden genoemd. UWV heeft verder enkele organisatorische maatregelen genomen, maar niet de nodige (en technische) maatregelen. Dit alles met een onvoldoende passend beveiligingsniveau tot gevolg.

3.5 Conclusie

De AP komt tot de conclusie dat UWV onvoldoende een op het risico afgestemd beveiligingsniveau gegarandeerd en gewaarborgd heeft in het kader van het verzenden van groepsberichten via de Mijn Werkmap-omgeving. Hierdoor was er sprake van een voortdurende overtreding waarbij UWV in de periode van 2012 tot en met 24 mei 2018 in strijd heeft gehandeld met artikel 13 van de Wbp en vanaf 25 mei 2018 tot december 2018 in strijd heeft gehandeld met artikel 32, eerste en tweede lid, van de AVG.

4. Boete

4.1 Inleiding

UWV heeft in strijd gehandeld met artikel 13 van de Wbp en artikel 32, eerste en tweede lid, van de AVG. De AP maakt voor de vastgestelde overtreding gebruik van haar bevoegdheid om aan UWV een boete op te leggen voor de periode van 1 januari 2016 (start boetebevoegdheid AP) tot december 2018. Gezien de ernst van de overtreding en de mate waarin deze aan UWV kan worden verweten, acht de AP de oplegging van een boete gepast. De AP motiveert dit in het navolgende.

Gezien er in dit geval sprake is van een voortdurende overtreding die zowel onder de Wbp als de AVG heeft plaatsgevonden, heeft de AP getoetst aan het materiële recht zoals dat gold op het moment waarop de gedraging plaatsvond. In dit geval is dat zowel artikel 13 van de Wbp als artikel 32, eerste en tweede lid, van de AVG. Deze bepalingen beogen dezelfde rechtsbelangen te waarborgen en er is geen (wezenlijke) materiële wijziging van de regelgeving op dit punt. Gezien dat het zwaartepunt van de overtreding zich bevindt ten tijde van de Wbp, ziet de AP in dit geval aanleiding om aan te sluiten bij de 'Boetebeleidsregels Autoriteit Persoonsgegevens 2016'.

4.2 Boetebeleidsregels Autoriteit Persoonsgegevens 2016

De AP hanteert in dit geval de 'Boetebeleidsregels Autoriteit Persoonsgegevens 2016' (Boetebeleidsregels) voor de invulling van de bevoegdheid tot het opleggen van een bestuurlijke boete, waaronder het bepalen van de hoogte daarvan.[57] In de Boetebeleidsregels is gekozen voor een categorie-indeling en bandbreedte systematiek.

Overtreding van artikel 13 van de Wbp is ingedeeld in categorie II. Categorie II heeft een boetebandbreedte tussen € 120.000 en € 500.000. Binnen de bandbreedte stelt de AP een basisboete vast. Als uitgangspunt geldt dat de AP de basisboete vaststelt op 33% van de bandbreedte van de aan de overtreding gekoppelde boetecategorie.[58] In dit geval wordt de basisboete vastgesteld op € 245.400.

4.3 Boetehoogte

De hoogte van de boete stemt de AP af op de factoren die zijn genoemd in artikel 6 van de Boetebeleidsregels, door het basisbedrag te verlagen of verhogen. Het gaat om een beoordeling van de ernst van de overtreding in het specifieke geval, de mate waarin de overtreding aan de overtreder kan worden verweten en, indien daar aanleiding toe bestaat, andere omstandigheden zoals de (financiële) omstandigheden waarin de overtreder verkeert.

[57] Beleidsregels van de Autoriteit Persoonsgegevens van 15 december 2015, zoals laatstelijk gewijzigd op 6 juli 2016, met betrekking tot het opleggen van bestuurlijke boetes (Boetebeleidsregels Autoriteit Persoonsgegevens 2016), *Stcrt.* 2016, 2043.
[58] Boetebeleidsregels, p. 10-11.

4.3.1 Ernst van de overtreding

Elke verwerking van persoonsgegevens dient behoorlijk en rechtmatig te geschieden. Ter voorkoming dat organisaties met verwerkingen van persoonsgegevens inbreuk maken op de privacy van burgers is het van groot belang dat zij een op risico afgestemd beveiligingsniveau toepassen. Bij het bepalen van het risico voor de betrokkene zijn onder andere de aard van de persoonsgegevens en de omvang 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. Naarmate de 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 de persoonsgegevens. De AP heeft geconcludeerd dat UWV onvoldoende een op risico afgestemd beveiligingsniveau heeft gegarandeerd en gewaarborgd in het kader van het verzenden van groepsberichten via de Mijn Werkmap-omgeving.

Voor wat betreft de aard van de gegevens heeft de AP vastgesteld dat UWV in Sonar een veelheid aan verschillende persoonsgegevens met een zeer gevoelig karakter verwerkt, waaronder gegevens over de gezondheid van personen en het BSN. Werkzoekenden, zieken en arbeidsongeschikten die wettelijk verplicht zijn zich te registreren bij UWV en daarvoor hun persoonsgegevens moeten verstrekken, moeten erop kunnen vertrouwen dat UWV op een deugdelijke wijze de risico's afweegt die deze personen lopen. De impact van een beveiligingsincident met de persoonsgegevens die UWV verwerkt kunnen groot zijn voor een omvangrijke groep personen. Zo kan het onvoldoende beveiligen van deze persoonsgegevens leiden tot stigmatisering of uitsluiting. Nu UWV ook het BSN verwerkt wat in de praktijk een koppeling van verschillende bestanden aanzienlijk vergemakkelijkt, bestaat er voor personen wiens gegevens in Sonar staan een extra risico op bedreiging van de persoonlijke levenssfeer.

Naast de gevoelige aard van de persoonsgegevens verwerkt UWV gegevens van ontzettend veel burgers. UWV verwerkte in Sonar in de periode van 2016 tot en met 2018 gegevens over gemiddeld 4.500.000 personen. Al deze mensen liepen risico's door het onvoldoende op risico afgestemd beveiligingsniveau van UWV. Bovendien heeft UWV al op meerdere momenten persoonsgegevens gelekt. Van in totaal 15.331 personen heeft UWV gegevens gelekt bij het verzenden van groepsberichten via de werkmap. Tot slot merkt de AP op dat de overtreding 2 jaar en 11 maanden heeft geduurd. De AP acht dit zeer ernstig.

Gelet op het bovenstaande ziet de AP, op grond van de mate van ernst van de overtreding, aanleiding om aan UWV een boete op te leggen en het basisbedrag van de boete te verhogen naar € 450.000.

4.3.2 Verwijtbaarheid

Volgens artikel 6, tweede lid, van de Beleidsregels houdt de AP rekening met de mate waarin de overtreding aan de overtreder kan worden verweten. Indien de overtreding opzettelijk is gepleegd of het gevolg is van ernstig verwijtbare nalatigheid als bedoeld in artikel 66, vierde lid, van de Wbp, wordt aangenomen dat sprake is van een aanzienlijke mate van verwijtbaarheid van de overtreder.

Blijkens de parlementaire geschiedenis is van 'ernstig verwijtbare nalatigheid' als bedoeld in artikel 66, vierde lid, van de Wbp sprake indien "*de overtreding het gevolg is van ernstig verwijtbare nalatigheid, dat wil zeggen*

het gevolg is van grof, aanzienlijk onzorgvuldig, onachtzaam dan wel onoordeelkundig handelen."[59] In dit verband wordt opgemerkt dat onder "*handelen*" als hiervoor bedoeld, ook een nalaten wordt verstaan.[60]

UWV is van mening dat uit de bevindingen van de AP niet volgt dat er sprake is van ernstige verwijtbare nalatigheid. De eerste vier datalekken waren voor UWV aanleiding om stevige aanpassingen in het proces door te voeren en in te zetten op bewustwording van de risico's bij handmatige verwerkingen. Volgens UWV is er tussen het vijfde en het achtste datalek ingezet op het verstevigen van deze organisatorische maatregelen (zoals workshops). Dit betekent volgens UWV dat er in het proces voor het versturen van groepsberichten in de Mijn Werkmap-omgeving wel degelijk is ingezet op maatregelen om de beveiliging te verbeteren.

De AP volgt deze zienswijze van UWV niet en motiveert dit als volgt. UWV is verplicht om een beveiligingsniveau te hanteren die passend is voor de aard en omvang van de verwerkingen die UWV uitvoert. Nu UWV jarenlang geen passend beveiligingsniveau heeft gewaarborgd, is de AP van oordeel dat UWV ernstig nalatig is geweest in het niet afwegen van risico's voor burgers, het treffen van passende beveiligingsmaatregelen en controleren en aanpassen van deze maatregelen. Voor de organisatorische maatregelen die volgens UWV wel zijn doorgevoerd, heeft UWV deze maatregelen niet gebaseerd op risicoafwegingen en hoe daarbij is stilgestaan met de mogelijke gevolgen voor de betrokkenen. Ook heeft UWV aangegeven dat zij niet heeft gecontroleerd of de getroffen maatregelen na de datalekken daadwerkelijk zijn ingevoerd en geëvalueerd.

De Wbp, de AVG en de CBP-richtsnoeren ten aanzien van de beveiliging van de verwerking van persoonsgegevens hebben uitdrukkelijk beschreven dat organisaties een op risico afgestemd beveiligingsniveau moeten hanteren. Van UWV mag mede gelet op de gevoelige aard en de grote omvang van de verwerking wel worden verwacht dat zij zich van de voor haar geldende normen vergewist en daar naar handelt.

Daarnaast vindt de AP het zeer onachtzaam en nalatig dat UWV pas na negen datalekken in december 2018 is overgegaan tot het doorvoeren van technische maatregelen. Namelijk het blokkeren van de mogelijkheid tot het toevoegen van onder andere Excel-bestanden bij het verzenden van groepsberichten via de Mijn werkmap-omgeving. Burgers die verplicht worden om persoonsgegevens af te staan moeten ervan uit kunnen gaan dat het UWV als overheidsinstantie meteen de nodige maatregelen neemt om hun persoonsgegevens goed te beschermen.

Het feit dat UWV ook niet heeft voldaan aan de eigen beleidsregels acht de AP mede verwijtbaar. Ondanks dat het beleid van UWV aangeeft dat men maatregelen moet nemen op basis van expliciete risicoafwegingen als onderdeel van een PDCA-cyclus, heeft UWV niet en onvoldoende rekening gehouden met de risico's en gevolgen voor werkzoekenden. Daarnaast heeft UWV pas in december 2018 een technische maatregel ingevoerd terwijl UWV op 20 oktober 2016 al had besloten om op korte termijn een onderzoek te starten naar de mogelijkheid tot het nemen van technische maatregelen. Ook heeft het UWV

[59] *Kamerstukken II* 2014/15, 33662, nr. 16, p. 1.
[60] *Handelingen II* 2014/15, 51, item 9, p. 11.

niet gecontroleerd of de maatregelen die wel zijn genomen naar aanleiding van de datalekken wel daadwerkelijk zijn ingevoerd in de organisatie. De overtreding is daarmee het gevolg van grof en aanzienlijk onzorgvuldig handelen door UWV.

Naar het oordeel van de AP blijkt uit al het bovenstaande dat UWV grof, aanzienlijk onzorgvuldig dan wel onachtzaam heeft gehandeld, waardoor sprake is van ernstige verwijtbare nalatigheid aan de zijde van UWV. Gelet op de omstandigheden van dit geval en het criterium van ernstig verwijtbare nalatigheid onder de Wbp ziet de AP echter geen aanleiding om het boetebedrag te verlagen of verder te verhogen.

4.3.3 Evenredigheid

Tot slot beoordeelt de AP op grond van het in artikel 5:46 van de Algemene wet bestuursrecht gecodificeerde evenredigheidsbeginsel of de toepassing van haar beleid voor het bepalen van de hoogte van de boete gezien de omstandigheden van het concrete geval, niet tot een onevenredige uitkomst leidt.

De AP is van oordeel dat, gezien de ernst van de overtreding en de mate waarin deze aan UWV kan worden verweten, (de hoogte van) de boete evenredig is.[61] De organisatorische maatregelen die volgens UWV wel zijn getroffen, nemen volgens de AP de onderhavige inbreuk op artikel 13 van de Wbp en artikel 32, eerste en tweede lid, van de AVG niet weg. Het niet afwegen van risico's voor burgers, het ontbreken van passende beveiligingsmaatregelen en het niet controleren en evalueren van deze maatregelen hebben immers geleid tot een onvoldoende op risico afgestemd beveiligingsniveau. De overtreding heeft daarnaast bijna 3 jaar geduurd waarbij de privacy van 4.500.000 personen onvoldoende gewaarborgd was.

Gezien alle omstandigheden van dit geval ziet de AP geen aanleiding het bedrag van de boete op grond van de evenredigheid en de in de Boetebeleidsregels genoemde omstandigheden, voor zover van toepassing in het voorliggende geval, nog verder te verhogen of te verlagen.

4.4 Conclusie

De AP stelt het totale boetebedrag vast op € 450.000-.

[61] Zie voor de motivering paragraaf 4.3.1 en 4.3.2.

Datum
31 mei 2021

Ons kenmerk
[VERTROUWELIJK]

5. Dictum

De AP legt aan het Uitvoeringsinstituut werknemersverzekeringen wegens overtreding van artikel 13 van de Wbp en artikel 32, eerste en tweede lid, van de AVG een bestuurlijke boete op ten bedrage van **€ 450.000** (zegge vierhonderdvijftigduizend euro).[62]

Hoogachtend,
Autoriteit Persoonsgegevens,

w.g.

drs. C.E. Mur
Bestuurslid

Rechtsmiddelenclausule
Indien u het niet eens bent met dit besluit kunt u binnen zes weken na de datum van verzending van het besluit digitaal of op papier een bezwaarschrift indienen bij de Autoriteit Persoonsgegevens. Het indienen van een bezwaarschrift schort de werking van dit besluit op. Voor het indienen van digitaal bezwaar, zie www.autoriteitpersoonsgegevens.nl, onder het kopje 'Bezwaar maken', onderaan de pagina onder de kop 'Contact met de Autoriteit Persoonsgegevens'. Het adres voor het indienen op papier is: Autoriteit Persoonsgegevens, Postbus 93374, 2509 AJ Den Haag. Vermeld op de envelop 'Awb-bezwaar' en zet in de titel van uw brief 'bezwaarschrift'. Schrijf in uw bezwaarschrift ten minste:

- Uw naam en adres
- De datum van uw bezwaarschrift
- Het in deze brief genoemde kenmerk (zaaknummer); u kunt ook een kopie van dit besluit bijvoegen
- De reden(en) waarom u het niet eens bent met dit besluit
- Uw handtekening

Zie voor meer informatie: https://autoriteitpersoonsgegevens.nl/nl/bezwaar-maken

[62] De AP zal voornoemde vordering uit handen geven aan het Centraal Justitieel Incassobureau (CJIB).

Datum
31 mei 2021

Ons kenmerk
[VERTROUWELIJK]

Bijlage 1

1. Beleid van UWV

UWV heeft in de beleidsdocumenten "*Strategisch Beleid Informatiebeveiliging en Privacy (IB&P)*", die gelden voor de periode 2016-2020, opgenomen: "*dat management besluiten neemt op basis van een zorgvuldige afweging van de risico's*".[63] Ook staat daar het volgende: "*Afhankelijk van de uitkomsten van de analyses worden risico's door een adequaat stelsel van maatregelen geneutraliseerd of expliciet door een directeur geaccepteerd. Hiervan wordt een centrale registratie bijgehouden. UWV blijft er voor zorgen dat de continuïteit, kwaliteit en veiligheid is geborgd. Dit betekent dat risico's vroegtijdig worden gedetecteerd en op een vakkundige wijze worden aangepakt*".[64]

Voorst heeft UWV in de beleidsdocumenten "*Tactisch Beleid, Informatiebeveiliging en Privacy (IB&P) Wettelijk Kader*", die golden vanaf april 2016 tot en met in ieder geval januari 2019, het volgende opgenomen: "*Bij de verwerking en opslag van persoonsgegevens worden de vereiste technische en organisatorische beveiligingsmaatregelen op een risico-gestuurde wijze geselecteerd en gerealiseerd, conform UWV Tactisch IB&P Beleid Sectie B 'BIR UWV'.*"[65]

UWV heeft in haar beleidsdocumenten, die golden vanaf april 2016 tot en met in ieder geval januari 2019, het volgende opgenomen: "*Bij de verwerking en opslag van persoonsgegevens worden de vereiste technische en organisatorische beveiligingsmaatregelen op een risico-gestuurde wijze geselecteerd en gerealiseerd, conform UWV Tactisch IB&P Beleid Sectie B 'BIR UWV'.*[66]

Ten aanzien van het controleren, evalueren en aanpassen van maatregelen stelt UWV in haar beleidsdocument, geldend van december 2015 tot in ieder geval januari 2019:[67]
"4.2. De organisatieonderdelen: primaire actoren
IB&P-risicomanagement is primair belegd bij de organisatieonderdelen zelf. Hierover dient binnen de eigen lijn te worden gerapporteerd, conform de eigen gemaakte afspraken. Vanuit de centrale bewaking van de IB&P-risico's worden de organisatieonderdelen gevraagd over de UWV-brede top IB&P-risico's te rapporteren.
De organisatieonderdelen hebben hierbij de volgende verantwoordelijkheden:

- *Rapporteren vanuit de uitvoeringsverantwoordelijkheid over de voortgang van deze geprioriteerde maatregelen en verbeteracties (met behulp van een format) en eventuele nieuwe IB&P-risico's via de divisierapportage;*
- *Periodiek herijken van de (BIR) verbeterplannen met daarin verbeteracties op basis van de UWV-breed vastgestelde IB&P-risico's;*

[63] Zie dossierstuk 38 (Excel-bestand, bijlage 6 (bestand "UWV BZ IBP Strategische Beleid v190", p. 7) en bijlage 11 (bestand "UWV BZ IBP Strategisch Beleid v202 (AVG-versie)", p 7-8). Deze bijlagen zijn onderdeel van bestand "Document" bij antwoord op vraag 4 onder datalek 1).
[64] Idem.
[65] Zie dossierstuk 38 (Excel-bestand, bijlage 7 (bestand "UWV BZ IBP Sectie A Wettelijk Kader v100.docx", p. 11) en bijlage 10 (bestand "UWV BZ IBP Sectie A Wettelijk Kader v102 (AVG-versie)", p. 12). Deze bijlagen zijn onderdeel van bestand "Document" bij antwoord op vraag 4 onder datalek 1).
[66] Zie dossierstuk 38 (Excel-bestand, bijlage 7 (bestand "UWV BZ IBP Sectie A Wettelijk Kader v100.docx", p. 11) en bijlage 10 (bestand "UWV BZ IBP Sectie A Wettelijk Kader v102 (AVG-versie)", p. 12). Deze bijlagen zijn onderdeel van bestand "Document" bij antwoord op vraag 4 onder datalek 1).
[67] Zie dossierstuk 38 (Excel-bestand, bijlage 9 (bestand "UWV BZ IBP Sectie C Borging BIR Beheersing v200" dat onderdeel is van bestand "Document" bij antwoord op vraag 4 onder datalek 1, p. 7-8)).

- *Op basis van de geprioriteerde UWV-brede IB&P-risico's en eigen risico-inventarisatie maatregelen doorvoeren en onderhouden (via de verbeterplannen).*

4.3. Bestuurszaken: coördinerende rol
De inhoudelijk ondersteuning en bewaking voor IB&P is centraal belegd bij Bestuurszaken.
Bestuurszaken is verantwoordelijk voor de coördinatie en het overall in beeld brengen van de IB&P-risico's. Voor het verkrijgen van het overallbeeld, voert Bestuurszaken de volgende activiteiten uit:

- *Bewaken van de voortgang en realisatie van acties en maatregelen op het terrein van IB&P, zoals voortgang op de verbeterplannen;*
- *Periodiek uitvoeren van een inhoudelijk kwalitatief onderzoek (Quality Assurance) naar de status van de IB&P verbeteracties en beheersing van de top IB&P-risico's bij de organisatieonderdelen;*
- *Opleveren van een IB&P-rapportage richting de Coalitie IB&P en de Raad van Bestuur, periodiek of bij bijzonderheden;*
- *Coördineren van de jaarlijkse exercitie van het herijken van de UWV-brede risico's en (BIR) verbeterplannen;*
- *Leveren van inhoudelijke ondersteuning over de uit te voeren verbeterplannen en acties;*
- *Actueel houden van het overzicht van de meest belangrijke UWV-brede IB&P-risico's".*[68]

2. Praktijk binnen UWV

2.1 Afwegen van risico's in de praktijk

UWV geeft ten aanzien van het uitvoeren van risicoanalyses aan dat zij: "*een organisatie is die in het algemeen en ook in het onderzoeken en voorkomen van datalekken, pragmatisch te werk gaat. UWV kiest voor een pragmatische aanpak met concrete verbeteringen in plaats van lijvige rapporten. Documenten die wij bijvoorbeeld als 'risicoanalyse' bestempelen, kunnen door het departement 'onderzoek' worden genoemd waardoor hetzij begrijpelijkerwijs maar onterecht de indruk kan ontstaan dat we niet volledig zijn".*[69]

Op de vraag of voorafgaand aan het besluit in 2012 om groepsberichten op andere wijze dan via Outlook te versturen een risicoanalyse is uitgevoerd, meldt UWV: "*Er is over het verzenden van groepsberichten via de werkmap geen risicoanalyse an sich gemaakt*".[70]

Op de vraag hoe UWV in 2012 heeft bepaald dat het verzenden van groepsberichten via de Mijn Werkmap-omgeving wel een acceptabel risico is, welke beveiligingsmaatregelen zijn overwogen en hoe die afweging is gemaakt, antwoordt UWV: "*De werkmap kent een koppeling met SONAR en werk.nl, en de klant dient door middel van zijn/haar DigiD in te loggen om berichten te kunnen openen en in te zien. Bovendien kunnen – in tegenstelling tot bij verzending via outlook- eenmaal verzonden berichten gewist worden, indien een bericht verkeerd verzonden is. UWV ziet de werkmap daarom als een van de veilige kanalen om gegevens en berichten mee uit te wisselen*".[71]

[68] Zie dossierstuk 38 (Excel-bestand, bijlage 9 (bestand "UWV BZ IBP Sectie C Borging BIR Beheersing v200" dat onderdeel is van bestand "Document" bij antwoord op vraag 4 onder datalek 1, p. 7-8)).
[69] Zie dossierstuk 46 (Beantwoording door UWV, bijlage 2 (bestand "Brief AP informatieverzoek 29042019", p. 1)).
[70] Zie dossierstuk 98 (Beantwoording door UWV, bestand "Aanvullende vragen AP2110", p. 2, bijlage 4 (bestand "Oplegnotitie vergadering Directieteam WERKbedrijf") en bijlage 5 (bestand "28 BV 06 Beslisdocument verbieden gebruik groepsmail via Outlook")).
[71] Zie dossierstuk 98 (Beantwoording door UWV, bestand "Aanvullende vragen AP2110", p. 2).

Op de vraag of de specifieke datalekken aanleiding zijn geweest tot het uitvoeren van een risicoanalyse geeft UWV aan: "*UWV en in het bijzonder de divisie WERKbedrijf heeft naar aanleiding van de vier lekken in 2016 een risicoanalyse uitgevoerd. Deze risicoanalyse vindt u terug in het document: 'Voorlegger DMO WERKbedrijf' en haar bijlagen, met daarin richtlijnen voor medewerkers*".[72] In deze voorlegger van oktober 2016 is het volgende opgenomen: "*Om de onrust het hoofd te bieden en de dienstverlening zo min mogelijk te verstoren, maar tegelijkertijd een grondige analyse te doen van waar wij in onze klantcommunicatie risico's lopen, stellen wij de volgende maatregelen voor* (…)".[73]

UWV heeft op de vraag of er na elk datalek een risicoanalyse is uitgevoerd het volgende aangegeven: "*Gedurende 2016 zag UWV geen noodzaak om een PIA als zodanig uit te voeren. De Business Security Officer (BSO) van Werkbedrijf heeft voor het Districtmanagers Overleg een evalutatie (sic) gemaakt n.a.v. de datalekken in augustus en september 2016. Zie hiervoor de voorlegger - een voorstel voor besluitvorming- van het 4e kwartaal 2016 van de BSO WERKbedrijf met hierin te nemen besluiten/impact analyse/maatregelen en conclusies en aanbevelingen. Daarnaast in de bijlage een richtlijn Veilig Communiceren bij WERKbedrijf. Doordat er in 2017 één lek was zag UWV geen noodzaak om het beleid aan te passen en wel een PIA uit te voeren. De Raad van bestuur heeft na de twee lekken in 2018 de Functionaris Gegevensbescherming gevraagd om een onderzoek te starten*".[74]

UWV geeft op de vraag waarom zij na het lek in 2017 geen noodzaak zag tot uitvoeren van een risicoanalyse het volgende aan: "*UWV heeft een afweging gemaakt en daarbij uiteraard ook gewicht toegekend aan de rechten en vrijheden van betrokkenen. Inmiddels, met de kennis van nu, deze afweging mogelijk anders zijn*".[75] UWV heeft desgevraagd geen stukken aangeleverd waarin de destijds gemaakte afweging is vastgelegd.

Ten aanzien van de datalekken vijf tot en met acht meldt UWV: "*Het risico op meer lekken werd als laag beschouwd en maatregelen uit oktober 2016 leken afdoende te werken, zoals we eerder toelichtten in de beantwoording van het informatieverzoek. Op dat moment kende een aantal andere ICT maatregelen in de systemen een hoge prioriteit. Achteraf bezien was dat een verkeerde inschatting en hadden technische maatregelen eerder moeten worden genomen*".[76] UWV heeft niet onderbouwd waarop de inschatting was gebaseerd dat het risico als laag diende te worden beschouwd.

UWV heeft in relatie tot het achtste datalek aangegeven: "*De Functionaris Gegevensbescherming (FG) heeft naar aanleiding van dit datalek een onderzoek uitgevoerd naar exportfunctionaliteit binnen de werkmap. Daarnaats (sic) voert de Functionaris Gegevensbescherming (FG) in opdracht van de Raad van Bestuur momenteel een risico-analyse uit op Sonar*".[77]

[72] Zie dossierstuk 46 (Beantwoording door UWV, bijlage 2 (bestand "Brief AP informatieverzoek 29042019", p. 1)).
[73] Zie o.a. dossierstuk 38 (Excel-bestand, bijlage 27 (bestand "Microsoft Word 97-2003-document" bij antwoord bij 11 onder datalek 1 t/m 4, p. 2)) en dossierstuk 102 (Beantwoording door UWV, bijlage 2 (bestand "42DMO-B04. 161017 ES Notitie DMO WB", p.2)).
[74] Zie o.a. dossierstuk 38 (Excel-bestand, antwoord bij 11 onder datalek 1 t/m 4).
[75] Zie dossierstuk 81 (Beantwoording door UWV, bijlage 1 (bestand "Beantwoording vragen AP augustus 2019", antwoord op vraag 12)).
[76] Zie dossierstukken 65 en 66 (Beantwoording door UWV, p. 2).
[77] Zie o.a. dossierstuk 38 (Excel-bestand, antwoord bij 11 onder datalek 7).

2.2 Maatregelen, controle en aanpassingen in de praktijk

Tijdelijke maatregelen van 28 september 2016

UWV stelt dat het noodzakelijk was de maatregelen die golden voorafgaande aan het vierde datalek te evalueren en dat zij heeft besloten tot het nemen van maatregelen.[78]

UWV meldde met betrekking tot de maatregelen na de vier datalekken in 2016: "*Toen zijn direct organisatorische- en procesmatige maatregelen getroffen om de risico's op herhaling te mitigeren*".[79] Uit de voorlegger van 18 oktober 2016 blijkt dat het "*DT WERKbedrijf*" op 28 september 2016 - na het vierde datalek - tot de volgende tijdelijke maatregelen had besloten, die betrekking hebben op het verzenden van berichten met bijlagen via de Mijn Werkmap-omgeving naar meerdere werkzoekenden tegelijk:[80]

> Sinds het ingaan van de Meldplicht Datalekken zijn bij WERKbedrijf 22 datalekken geregistreerd (zie bijlage C). Elk van deze datalekken heeft een flinke impact op de organisatie in termen van inzet van medewerkers, onderbreking van de reguliere bedrijfsvoering, imagoschade en mogelijke boetes en schadeclaims. Zij kosten de organisatie kortom veel geld. Maar nog belangrijker is dat met elk van deze datalekken klanten zijn gedupeerd. Klanten wiens persoonsgegevens door ons toedoen in de verkeerde handen terecht zijn gekomen terwijl wij juist geacht worden zeer zorgvuldig met deze gegevens om te gaan.
>
> In reactie hierop heeft het DT op 28 september 2016 tot een tijdelijke voorzorgsmaatregel besloten om datalekken te voorkomen:
>
> *Het is tot nader order pas mogelijk om een extern bericht aan meerdere werkzoekenden /gemeenten/werkgevers te versturen indien:*
>
> - *er akkoord is gegeven door het management (Districtsmanager/regiomanager/manager werkzoekendendienstverlening of manager werkgeversdienstverlening);*
> - *deze ook toeziet op de allerlaatste versie van het te verzenden bulkbericht;*
> - *er alleen gewerkt wordt met een 'gestripte Excellijst'. Dat is een Excellijst waarin geen kolommen met overbodige persoonsgegevens staan, zoals namen, burgerservicenummers (BSN's), leeftijden, woongemeenten en postcodes van klanten. Gebruik als het even kan bij de verzending alleen een Excellijst waarin de 'ROW_ID'-kolom staat. Dat is een kolom die Sonar herkent en waarin codes staan waarmee klanten worden opgegeven als geadresseerden;*
> - *er altijd twee paar ogen meekijken.*
>
> *Berichten naar werkzoekenden worden uitsluitend via de werkmap verstuurd.*

Op 30 september 2016 zijn deze tijdelijke maatregelen en de instructies gecommuniceerd aan de managers van het WERKbedrijf via het volgende WERKbericht:[81]

[78] Zie o.a. dossierstuk 38 (Excel-bestand, antwoord op vraag 18 onder datalek 1 t/m 4).
[79] Zie dossierstukken 65 en 66 (Beantwoording door UWV, p. 1).
[80] Zie dossierstukken 65 en 66 (Beantwoording door UWV, bijlage, antwoord op vraag 2) en dossierstuk 102 (Beantwoording door UWV), bijlage 2 (bestand "42DMO-B04. 161017 ES Notitie DMO WB", p.1).
[81] Zie dossierstuk 98 (Beantwoording door UWV, bijlage 2 (bestand "Werkbericht 30 september 2016", p. 2 en 3)).

02. Versturen bulkberichten aan banden

Als gevolg van een recent datalek in de regio Groningen, gelden er vanaf nu voor het hele land belangrijke voorzorgsmaatregelen om nieuwe datalekken te voorkomen. Lees meer over het datalek in Groningen op intranet.

De volgende regels gelden vanaf nu:

- Tot nader order mag een medewerker geen bulkberichten/mailing (>2 ontvangers) versturen.
- Een mailing is alleen mogelijk wanneer:
  - Er akkoord is gegeven door management.
  - De manager ook toeziet op de finale e-mail.
  - Er alleen wordt gewerkt met een gestripte Excellijst, waaruit eerst alle kolommen die niet nodig zijn, zijn verwijderd.
  - Altijd twee paar ogen meekijken.
- Er mogen geen e-mails via Outlook (onveilige verbinding) naar werkzoekenden worden gestuurd, alleen via de Werkmap.

UWV stelt dat deze tijdelijke maatregelen en de instructies op 4 oktober 2016 zijn gecommuniceerd aan alle (toen in dienst zijnde) medewerkers via een nieuwsbrief WERKInUitvoering met de volgende tekst:[82]

Wat houdt de strengere voorzorgsmaatregel in?
Als gevolg van het datalek in Groningen geldt tijdelijk voor alle vestigingen in het land dat het alleen onder strikte voorwaarden is toegestaan om een bulkbericht te verzenden. Het is tot nader order pas mogelijk om een extern bericht aan meerdere werkzoekenden/gemeenten/werkgevers te versturen indien:
- er akkoord is gegeven door het management (Districtsmanager/regiomanager/manager werkzoekendendienstverlening of manager werkgeversdienstverlening);
- deze ook toeziet op de allerlaatste versie van het te verzenden bulkbericht;
- er alleen gewerkt wordt met een 'gestripte Excellijst'. Dat is een Excellijst waarin geen kolommen met overbodige persoonsgegevens staan, zoals namen, burgerservicenummers (BSN's), leeftijden, woongemeenten en postcodes van klanten. Gebruik als het even kan bij de verzending alleen een Excellijst waarin de 'ROW_ID'-kolom staat. Dat is een kolom die Sonar herkent en waarin codes staan waarmee klanten worden opgegeven als geadresseerden;
- er altijd twee paar ogen meekijken.

Deze maatregelen zijn tijdelijk en worden na een lopend onderzoek vervangen door maatregelen voor de langere termijn.

UWV geeft over op de vorige bladzijde genoemde tijdelijke maatregelen aan dat deze zo snel als mogelijk na 28 september 2016 in werking zijn getreden. Ook stelt UWV dat gezien het belang van deze maatregelen en de relevantie voor het type risico's dat vooral speelt bij dit soort datalekken, deze tijdelijke maatregelen op dit moment nog steeds van kracht zouden zijn.[83] UWV heeft dit echter niet met stukken onderbouwd.

[82] Zie dossierstuk 98 (Beantwoording door UWV, bijlage 3 (bestand "WIU 4 oktober 2016")).
[83] Zie dossierstukken 65 en 66 (Beantwoording door UWV, bijlage, antwoord op vraag 2).

Maatregelen die in oktober 2016 zijn voorgesteld

In de voorlegger van 18 oktober 2016 die is opgesteld ter voorbereiding van het Districtsmanagers overleg (DMO) op 20 oktober 2016 staat het volgende over de hierboven genoemde tijdelijke maatregelen:[84]

> Sinds de communicatie van deze maatregel zijn er uit de districten veel reacties gekomen. Er leven veel vragen over wat er wel en niet mag, er is onrust over hoe (met name werkgevers- en AG-) dienstverlening nu verder moet, en her en der maakt men het zichzelf onnodig extra moeilijk. Er is bij een flink aantal regio's weinig vertrouwen in de effectiviteit van de werkmap. Tegelijkertijd zijn er ook regio's die aangeven dat zij allang alleen via de werkmap met klanten communiceren, ook in geval van berichten aan groepen klanten.
> Daarnaast valt op dat er veel van technische maatregelen wordt verwacht, terwijl het in alle gevallen om **menselijke fouten** gaat, die niet of slechts gedeeltelijk technisch kunnen worden voorkomen.

Daarom is het DMO in oktober 2016 gevraagd akkoord te gaan met onderstaande maatregelen, ter vervanging van de tijdelijke maatregelen waartoe op 28 september 2016 was besloten:[85]

Voorgestelde Maatregelen
Om de onrust het hoofd te bieden en de dienstverlening zo min mogelijk te verstoren, maar tegelijkertijd een grondige analyse te doen van waar wij in onze klantcommunicatie risico's lopen, stellen we de volgende maatregelen voor op het gebeid van awareness, proces en ICT:

Zo spoedig mogelijk
1. Akkoord op richtlijn veilig communiceren bij WERKbedrijf → JZ, IM, DT/DMO
2. Communiceren over veilig omgaan met gegevens en de richtlijn veilig communiceren bij WERKbedrijf *(awareness, proces)* → actie DMO en communicatie, mogelijk versterkt door een persoonlijke e-mail van Tof;
3. Per Arbeidsmarktregio één persoon benoemen die zich specifiek met veilige communicatie bezig houdt en deze inzetten bij de implementatie van de rest van de voorgestelde maatregelen. Dit zou bijvoorbeeld de klantcoördinator kunnen zijn *(proces)* → actie DMO;
4. Tijdelijke werkgroep instellen die richtlijn aanvult met casuïstiek en een Q en A voor de uitvoering bijhoudt. *(awareness, proces)* → actie IM, Bedrijfsvoering, Communicatie WB, LTI en vertegenwoordiging vanuit uitvoering (bijvoorbeeld zoals onder punt 3 benoemd);
5. Werkproces opstellen om bulkmail bij de dienst Peopleworks aan te leveren *(proces)* → actie OBW/EDW en Communicatie WB.
6. Toolkit op de implementatie pagina maken waarin alle informatie over de maatregelen wordt aangeboden *(proces)* → actie IM en LTI

Korte termijn:
7. In districten de lokale werkwijzen tegen het licht houden:
   a. Detectie van mogelijk verborgen bedreigingen (dit naar aanleiding van het recente datalek dat werd veroorzaakt door een lokaal monitorproces van proefplaatsingen);
   b. Toetsen op de richtlijn veilig communiceren bij WERKbedrijf;
   c. Kritische blik op wenselijkheid/effectiviteit van bulkmail.

   (proces) → actie DMO. Voorstel is om hiervoor de onder punt 3 benoemde medewerker bij in te zetten;
8. Veilige omgang met gegevens prominenter op het programma van de workshops integriteit plaatsen *(awareness)* → actie IM, Bureau Integriteit;
9. Meldplicht Datalekken nog nadrukkelijker opnemen in de IB&P gesprekken op de werkpleinen → actie Bedrijfsvoering;
10. Mogelijkheden technische maatregelen onderzoeken:
    a. Technisch onmogelijk maken om Excellbestanden aan een werkmapbericht toe te voegen;
    b. Matchingsproces faciliteren door WWO import en Beroepen- en opleidingenbrowser aan te passen;
    c. Notificatiemails te voorzien van een onderwerpsveld.

    (ICT) → actie OBW/EDW en IM

Middellange termijn:
11. Eens per kwartaal terugkoppeling (monitoring) over ontwikkeling datalekken in DMO *(awareness)* → actie IM/DMO
12. Veilige omgang met gegevens terugkerend onderwerp bij overleggen in de districten *(awareness)* → actie DMO
13. Veilige omgang met gegevens onderdeel laten uitmaken van management contract en de HRM-cyclus → actie DT en HRM

[84] Zie dossierstuk 102 (Beantwoording door UWV, bijlage 2 (bestand "42DMO-B04. 161017 ES Notitie DMO WB", p.2)).
[85] Zie dossierstuk 102 (Beantwoording door UWV, bijlage 2 (bestand "42DMO-B04. 161017 ES Notitie DMO WB", p. 2)).

Tijdens het DMO van 20 oktober 2016 is ten aanzien van de hierboven voorgestelde maatregelen het volgende besloten:[86]

161020-B4	**Datalek** – [redacted] *Aanwezig:* Helaas is het issue datalek nog steeds actueel. DMO geeft akkoord op de voorgestelde maatregelen. Maatregel 1 t/m 6 wordt zo spoedig mogelijk opgepakt. Dit zijn de volgende maatregelen: 1. Akkoord op richtlijn veilig communiceren bij WERKbedrijf → JZ, IM, DT/DMO 2. Communiceren over veilig omgaan met gegevens en de richtlijn veilig communiceren bij WERKbedrijf *(awareness, proces)* → actie DMO en communicatie, mogelijk versterkt door een persoonlijke e-mail van Tof; 3. Per Arbeidsmarktregio één persoon benoemen die zich specifiek met veilige communicatie bezig houdt en deze inzetten bij de implementatie van de rest van de voorgestelde maatregelen. Dit zou bijvoorbeeld de klantcoördinator kunnen zijn *(proces)* → actie DMO (coördinator klantbejegening?); 4. Tijdelijke werkgroep instellen die richtlijn aanvult met casuïstiek en een Q en A voor de uitvoering bijhoudt. *(awareness, proces)* → actie IM, Bedrijfsvoering, Communicatie WB, LTI en vertegenwoordiging vanuit uitvoering (bijvoorbeeld zoals onder punt 3 benoemd); 5. Werkproces opstellen om bulkmail bij de dienst Peopleworks aan te leveren *(procesbeschrijving)* → actie OBW/EDW en Communicatie WB. 6. Toolkit op de implementatie pagina maken waarin alle informatie over de maatregelen wordt aangeboden *(proces)* → actie IM en LTI Maatregel 7 t/m 10 wordt op korte termijn opgepakt. Op korte termijn volgt hier een voorstel met advies en termijn. Dan komt het terug in het DMO. Maatregel 11 t/m 13 wordt op de middellange termijn opgepakt. Het belang van een goede samenwerking tussen de afdelingen op het HK (IM, OBW en EDW) wordt benadrukt.	DM

Uit deze notulen volgt dat het DMO op 20 oktober 2016 alleen met de (op pagina 30 genoemde) maatregelen 1 tot en met 6 akkoord is gegaan. Daarnaast is besloten dat maatregelen 7 tot en met 10 - waaronder een onderzoek naar concrete technische maatregelen - op korte termijn op te pakken.

UWV geeft aan dat alle (op pagina 30 genoemde) maatregelen zijn geïmplementeerd.[87] UWV heeft echter niet (voldoende) onderbouwd of en wanneer de implementatie heeft plaatsgevonden. Van de maatregelen 1 tot en met 6 heeft UWV alleen aangetoond dat de "Richtlijn veilig communiceren bij WERKbedrijf" is opgesteld.[88] Zoals hieronder te zien is, staan in deze - niet gedateerde - Richtlijn uitgangspunten voor veilig communiceren:[89]

[86] Zie dossierstuk 102 (Beantwoording door UWV, bijlage 1 (bestand "42DMO-A04. Besluiten en actiepuntenoverzicht 20 okt. 2016", p. 3 en 4)).
[87] Zie dossierstuk 38 (Excel-bestand, antwoord op vraag 14 onder datalek 1).
[88] Zie dossierstuk 38 (Excel-bestand, bijlage 33 (bestand "161020 Bijlage A Datalekken WB", dat onderdeel is van bestand "Microsoft Word-document" bij antwoord op vraag 15 onder datalek 1)).
[89] Zie dossierstuk 38 (Excel-bestand, bijlage 33 (bestand "161020 Bijlage A Datalekken WB", dat onderdeel is van bestand "Microsoft Word-document" bij antwoord op vraag 15 onder datalek 1)).

Bijlage A: Richtlijn veilig communiceren bij WERKbedrijf

Binnen WERKbedrijf werken we vanuit onze wettelijke taak veel met persoonsgegevens en communiceren wij met werkzoekenden, werkgevers, collega's en leveranciers. Zolang wij binnen het wettelijk kader blijven is dit geoorloofd, mits we ons daarbij ook houden aan de wetgeving ter bescherming van persoonsgegevens (Wet Bescherming Persoonsgegevens).

Om een handreiking te doen wat je dan wel en niet kan en mag doen in onze dienstverlening, zijn onderstaande uitgangspunten geformuleerd. Deze uitgangspunten zijn niet bedoeld om onze dienstverlening te verlammen, maar juist om ons in staat te stellen om een bewuste afweging te maken hoe wij de dienstverlening op een zo veilig mogelijke manier kunnen uitvoeren, waarbij de privacy van burgers zo min mogelijk wordt geschonden.

Uitgangspunten:

1. Kies bij het uitvoeren van een taak waarbij je persoonsgegevens verwerkt altijd voor de manier die het minste de privacy van burgers schendt;
   ➔ Kies niet voor makkelijkst of snelst; maar bekijk kritisch of er een veiliger alternatief is.
2. Als je voor het uitvoeren van je taak persoonsgegevens moet delen, kies dan voor een veilige manier van communiceren.
   ➔ Extern: Werkmap en fysieke post wordt als veilig beschouwd; e-mail via Outlook niet.
   ➔ Outlook is binnen de SUWI-keten een beveiligd communicatiemiddel, mits verantwoord gebruikt.
3. Maak zo min mogelijk gebruik van foutgevoelige processtappen zoals het aanleggen en uploaden van bijlagen.

Uitwerking:

1. Minste schending van de privacy van burgers:
   - Wees alert op hoeveel personen je in je communicatie met en over klanten betrekt;
   - Wees kritisch op hoe je met gegevens omgaat; heb je de persoonsgegevens echt nodig voor het uitoefenen je taak? En hoe zit het met de collega's/externen met wie je de gegevens deelt; zijn de gegevens ook voor hen noodzakelijk?
   - Maak geen grote bestanden met klantgegevens aan, maar beperk je tot de rubrieken die je nodig hebt en houdt de deling van het bestand beperkt.
2. Als je voor het uitvoeren van je taak persoonsgegevens moet delen, kies dan voor een veilige manier van communiceren:
   - Gebruik altijd de werkmap voor het communiceren met werkzoekenden, ook wanneer je een groep wilt aanschrijven;
   - Indien je e-mailt, wees dan alert op automatische aanvulling in je Outlook adresbalk en het gebruik van BCC/CC;
   - Mail geen cv's naar werkgevers, maar wijs hen op de cv op werk.nl;
   - Verzend geen persoonsgegevens via e-mail naar re-integratiebedrijven, maar stuur de stukken per post;
   - Wanneer de klant ons via e-mail benadert, geef dan aan de klant aan dat hij voortaan via de werkmap moet communiceren.
3. Zo min mogelijk foutgevoelige processtappen:
   - Maak geen grote bestanden met klantgegevens aan, maar werk zoveel mogelijk binnen het systeem en sla geen bestanden op;
   - Als je toch een bestand met klantgegevens moet opslaan, doe dit dan in een aparte map/op een aparte schijf, die je alleen voor dit doeleinde gebruikt.

Uit pagina 30 en 31 volgt dat het DMO op 20 oktober 2016 heeft besloten een onderzoek naar de mogelijkheden van technische maatregelen uit te stellen tot nader order. Op de vraag of dit onderzoek heeft plaatsgevonden, heeft UWV geantwoord: "*Nee, dit onderzoek heeft niet plaatsgevonden*".[90]

UWV meldt met betrekking tot de vraag hoe is gecontroleerd of voorgestelde maatregelen na ieder datalek ook daadwerkelijk zijn ingevoerd: "*UWV en WERKbedrijf hebben niet als zodanig gecontroleerd of maatregelen die zijn genomen naar aanleiding van datalekken daadwerkelijk zijn ingevoerd. UWV heeft geen generiek beleid waarin het controleert of UWV-centrale maatregelen zijn geïmplementeerd door de verantwoordelijke divisie(s). Binnen divisies als*

[90] Zie dossierstukken 65 en 66 (Beantwoording door UWV, bijlage, p. 1, antwoord op vraag 3).

WERKbedrijf die door het hele land opereren kunnen regiokantoren tot op zekere hoogte eigen invulling geven aan centraal beleid, bijvoorbeeld bij bewustwordingscampagnes".[91] Tevens meldt UWV hierover: "*Er is geen formeel geprotocolleerde procedure binnen UWV waarbinnen er op centraal niveau wordt gecontroleerd of dergelijke afgesproken organisatorische- en procesmatige maatregelen worden uitgevoerd. Dat zou ondoenlijk zijn gezien de omvang van de organisatie en de hoeveelheid beslissingen die UWV neemt*".[92] UWV vermeldt als reactie op de feitelijke bevindingen echter dat zij wel degelijk gecontroleerd zou hebben of de genomen maatregelen in praktijk zijn gebracht.[93] Deze stelling heeft UWV niet onderbouwd met documentatie.

Op de vraag of en op welke wijze de maatregelen waartoe UWV naar aanleiding van eerste vier datalekken had besloten zijn geëvalueerd, wat de uitkomsten van die evaluatie waren en of het gewenste effect van die maatregelen was bereikt, meldt UWV: "*Nee, gezien het in absolute zin relatief beperkte aantal lekken uit 2017 t.o.v. 2016, zag UWV nog geen reden om aan te nemen dat de mitigerende maatregelen de risico's niet op juiste wijze adresseerden*".[94] En: "*In 2017 zag UWV gezien het relatief kleine aantal lekken (1), geen aanleiding om bestaande maatregelen te evalueren*".[95]

UWV stelt ten aanzien van de wijze waarop zij evaluaties uitvoert het volgende: "*Er is geen formeel geprotocolleerd evaluatieproces doorlopen na ieder van de zeven datalekken. Dat is niet de manier waarop UWV in alle gevallen werkt. Betrokken afdelingen concludeerden gedurende geruime tijd in goed overleg dat de in 2016 genomen maatregelen volstonden. Deze conclusie bleek achteraf helaas onjuist*".[96] UWV vermeldt als reactie op de feitelijke bevindingen echter dat er wel evaluaties zijn uitgevoerd met betrekking tot genomen maatregelen.[97] Deze stelling heeft UWV niet onderbouwd.

<u>Vijfde datalek</u>

UWV heeft aangegeven dat na het vijfde datalek verder is ingezet op het verhogen van de awareness bij het verzenden van berichten via de Mijn Werkmap-omgeving.[98] In dat kader is na het datalek op 20 juli 2017 door UWV het volgende WERKbericht verstuurd aan managers van het WERKbedrijf:[99]

[91] Zie dossierstuk 38 (Excel-bestand, antwoord op vraag 16 onder datalek 1 t/m 7).
[92] Zie dossierstukken 65 en 66 (Beantwoording door UWV, bijlage, p. 2, antwoord op vraag 4).
[93] Zie dossierstukken 109 en 116 (Reactie UWV op feitelijke bevindingen, p. 3).
[94] Zie o.a. dossierstuk 38 (Excel-bestand, antwoord op vraag 18 onder datalek 6).
[95] Zie o.a. dossierstuk 38 (Excel-bestand, antwoord op vraag 18 onder datalek 1 t/m 4).
[96] Zie dossierstukken 65 en 66 (Beantwoording door UWV, bijlage, p. 2, antwoord op vraag 5).
[97] Zie dossierstukken 109 en 116 (Reactie UWV op feitelijke bevindingen, p. 3).
[98] Zie o.a. dossierstuk 38 (Excel-bestand, antwoord op vraag 13 onder datalek 5).
[99] Zie dossierstuk 38 (Excel-bestand, bijlage 31 (bestand "Microsoft Word-document" bij antwoord op vraag 14 onder datalek 5)).

WERKbericht

Vooraankondiging activiteiten rond voorkomen datalekken

Om datalekken verder terug te dringen en awareness rond het veilig omgaan met persoonsgegevens verder te vergroten, heeft het team Informatiebeveiliging en Privacy (IB&P) met DT de volgende activiteiten afgesproken:

- Workshop Preventie datalekken
- Bezoek aan de districten
-

Beide initiatieven zullen met ingang van september van start gaan.

De workshop bestaat uit een informatieve presentatie en een interactief gedeelte waarin medewerkers zelf een risico analyse maken. Doel van de workshop is om meer kennis op te doen over veilig omgaan met persoonsgegevens en om meer bewustzijn te creëren over mogelijke risico's rond het werken met persoonsgegevens. De workshop wordt met een train de trainer sessie overgedragen aan de door de regio's aangedragen contactpersonen datalekken. Deze contactpersonen ontvangen hier volgende week een uitnodiging voor. Om de contactpersonen verder te faciliteren is een toolkitpagina ingericht met ondersteunend materiaal en blijft het IB&P team betrokken om ondersteuning te bieden. De overige medewerkers worden na de train de trainer sessies via de Werk in Uitvoering geïnformeerd over de workshop.

De bezoeken aan de districten hebben tot doel om het lokaal management bekend te maken met de organisatie van IB&P binnen WERKbedrijf en het beschikbare materiaal om in de regio's met awareness aan de slag te gaan. Daarnaast willen we met deze bezoeken een extra boost geven aan de uitrol van de workshops.

Vragen of meer informatie?

Ook stelt UWV met betrekking tot dit datalek: "*UWV/WERKbedrijf heeft als gevolg van dit lek de Richtlijn 'Veilig communiceren opgesteld*'" en heeft UWV de "Richtlijn veilig communiceren bij WERKbedrijf" bij de beantwoording van vragen over het vijfde datalek gevoegd.[100] Op basis van het genoemde op pagina 31 lijkt echter te volgen dat deze richtlijn reeds na het vierde datalek was opgesteld. En zoals reeds eerder vermeld, heeft UWV geen bewijs geleverd dat de maatregel daadwerkelijk is ingevoerd of gecontroleerd.

UWV geeft verder aan met betrekking tot het vijfde datalek in 2017: "*Van belang voor de beslissing om indertijd, na dit lek, geen extra technische maatregelen te nemen was vooral een volle release-agenda, in combinatie met een vergaande veranderopdracht voor WERKbedrijf*".[101] UWV heeft geen stukken aangeleverd waarin dit besluit is vervat.

UWV heeft met betrekking tot de vraag hoe is gecontroleerd dat de genoemde maatregelen ook daadwerkelijk zijn uitgevoerd geantwoord dat UWV en WERKbedrijf niet als zodanig hebben gecontroleerd of maatregelen die zijn genomen naar aanleiding van datalekken daadwerkelijk zijn ingevoerd.[102]

[100] Zie o.a. dossierstuk 38 (Excel-bestand, antwoord op vraag 18 onder datalek 5).
[101] Zie dossierstuk 81 (Beantwoording door UWV, bijlage 1 (bestand "Beantwoording vragen AP augustus 2019"), antwoord op vraag 12).
[102] Zie dossierstuk 38 (Excel-bestand, antwoord op vraag 16 onder datalek 1 t/m 7).

Op de vraag of en op welke wijze de maatregelen waartoe UWV na het vijfde datalek had besloten zijn geëvalueerd, wat de uitkomsten van die evaluatie waren en of het gewenste effect van die maatregelen was bereikt, meldt UWV: "*Nee er heeft geen evaluatie plaatsgevonden na dit lek omdat het als incident werd beschouwd waarvoor de mitigerende maatregelen op dat moment effectief leken*".[103]

UWV stelt ten aanzien van de wijze waarop zij evaluaties van maatregelen uitvoert het volgende: "*Er is geen formeel geprotocolleerd evaluatieproces doorlopen na ieder van de zeven datalekken. Dat is niet de manier waarop UWV in alle gevallen werkt. Betrokken afdelingen concludeerden gedurende geruime tijd in goed overleg dat de in 2016 genomen maatregelen volstonden. Deze conclusie bleek achteraf helaas onjuist*".[104] UWV vermeldt als reactie op de feitelijke bevindingen echter dat er wel evaluaties zijn uitgevoerd met betrekking tot genomen maatregelen.[105] Deze stelling dat er wel geëvalueerd zou zijn wordt niet onderbouwd met documentatie waaruit de evaluatie daadwerkelijk blijkt.

Zesde tot en met negende datalek (2018)

UWV heeft aangegeven dat naar aanleiding van het zesde datalek op 26 maart 2018 geen maatregelen zijn getroffen.[106] Volgens UWV is na het zevende datalek op 28 maart 2018 en het achtste datalek op 3 augustus 2018, tot de volgende maatregelen besloten:[107]

"- ***Workshop Preventie Datalekken***
Dit betreft een workshop die gericht is op het vergroten van het bewustzijn rond het werken met persoonsgegevens en het samen uitvoeren van risicoanalyses. De workshop is via het 'train de trainer' overgedragen aan vertegenwoordigers uit alle arbeidsmarktregio's, die vervolgens de training hebben uitgerold over de vestigingen.
- ***Veelgebruikte toolkitpagina op DWU***
Mede naar aanleiding van de introductie AVG is de toolkitpagina van het IB&P verder uitgebreid en is er veel materiaal aangeboden. Dit deels ter ondersteuning van bovengenoemde workshop.
- ***Stappenplan Veilig Persoonsgegevens delen***
In het licht van de inwerkingtreding van de AVG is de oude richtlijn 'Veiliger Digitaal Communiceren' vervangen door de richtlijn 'Stappenplan Veilig Persoonsgegevens delen'
- ***Aandacht bij het management***
Met het regiomanagement vindt jaarlijks het adviesgesprek Informatiebeveiliging & Privacy en Veiligheid plaats. Ook loopt er momenteel een UWV brede IB&P training voor managers met daarin een breakoutsessie 'datalekken en rol management daarbij'
- ***Uitrol SLIM***
Bij de uitrol van SLIM werken is veel er aandacht voor veilig werken en het voorkomen van datalekken. Dit zowel tijdens MT-sessies, als ook tijdens vestiging brede kick-offs.
Technische maatregel:

[103] Zie o.a. dossierstuk 38 (Excel-bestand, antwoord op vraag 18 onder datalek 5).
[104] Zie dossierstukken 65 en 66 (Beantwoording door UWV, bijlage, p. 2, antwoord op vraag 5).
[105] Zie dossierstukken 109 en 116 (Reactie UWV op feitelijke bevindingen, p. 3).
[106] Zie dossierstuk 81 (Beantwoording door UWV, bijlage 3 (bestand "Vraag 7 bijlage 2")).
[107] Zie o.a. dossierstuk 38 (Excel-bestand, antwoord op vraag 13 onder datalek 6 en 7).

*Bijlagen-**blokkade***
WERKbedrijf heeft het doormiddel van een vervroegde release in het weekend van 15/16 december 2019 (sic) onmogelijk gemaakt om nog langer o.a. Excel-bestanden in de Werkmap bij te voegen aan berichten."

Met uitzondering van de maatregel ten aanzien van het "Stappenplan Veilig Persoonsgegevens delen" en de technische maatregel heeft UWV geen documenten of een nadere onderbouwing aangeleverd op basis waarvan kan worden vastgesteld hoe de hierboven genoemde maatregelen zijn geborgd in documentatie. Verder is niet duidelijk geworden wanneer bovengenoemde maatregelen zijn geïmplementeerd.

UWV heeft een versie van het "*Stappenplan Veilig Persoonsgegevens delen"* aangeleverd. Dat stappenplan is gedateerd op 26 april 2018 en dus na het zevende datalek opgesteld. UWV verklaart hierover: "*In het licht van de inwerkingtreding van de AVG is de oude richtlijn 'Veiliger Digitaal Communiceren' vervangen door de richtlijn 'Stappenplan Veilig Persoonsgegevens delen".*[108] Dit stappenplan ziet er als volgt uit:

[108] Zie dossierstuk 38 (Excel-bestand, antwoord op vraag 13 onder datalek 6 en 7).

Stappenplan Veilig Persoonsgegevens delen

	Vraag en omschrijving
	**Waarom** wil ik persoonsgegevens delen? Wat is mijn doel? *Persoonsgegevens mogen alleen verwerkt worden als je goed kunt uitleggen wat daar het doel van is. Je mag geen gegevens die je voor één doel hebt verzameld voor een ander doel inzetten. Bijvoorbeeld: lijst klanten workshop gebruiken voor aanleveren kandidaten voor vacature aan werkgever*
	Past dat doel bij onze **wettelijke taak**? *Persoonsgegevens mogen bij UWV alleen worden gebruikt als dit noodzakelijk is voor het uitvoeren van onze wettelijke taak. WERKbedrijf heeft de wettelijke taak om mensen aan het werk te helpen en te houden. Hieronder vallen de volgende werkzaamheden:* • *Re-integratie van personen en arbeidsbemiddeling* • *Registratie van werkzoekenden en vacatures* • *Indicatie WSW* • *Transparantie van de arbeidsmarkt* ***Deel alleen persoonsgegevens als dit noodzakelijk is voor het uitvoeren van je wettelijke taak***
	**Welke gegevens** wil ik delen? *Persoonsgegevens zijn alle gegevens die tot een natuurlijk persoon herleidbaar zijn, zoals bijvoorbeeld de naam, adres, woonplaats, e-mail of telefoonnummer, enz.* *Daarnaast kennen we **bijzondere persoonsgegevens** zoals:* • *gegevens over gezondheid (persoonsgegevens over de fysieke of mentale gezondheid van een persoon. Denk hierbij aan: gewicht, hartslag, handicap, ziekterisico of verleende gezondheidsdiensten);* • *strafrechtelijk verleden.* ***Met bijzondere persoonsgegevens moet vanwege hun gevoelige aard extra voorzichtig worden omgegaan.***
	Zijn alle persoonsgegevens die je wilt delen **strikt noodzakelijk** voor het doel? *Bijvoorbeeld: wanneer je persoonsgegevens doorgeeft aan een samenwerkingspartner zodat hij contact op kan nemen met de klant, deel je alleen de naam en het telefoonnummer. Met die gegevens kan het doel bereikt worden.* ***Schrap alles wat niet strikt noodzakelijk is om het doel te bereiken***
	**Met wie** ga ik deze persoonsgegevens delen? • *Mag die persoon/instantie deze gegevens inzien op basis van haar wettelijke taak?* • *Welke afspraken hebben we met die persoon/instantie over het gebruik van de gegevens?* ***Deel alleen als de ander ook met deze persoonsgegevens mag werken***
	**Hoe** ga ik de gegevens delen? • *Is er een beveiligde omgeving beschikbaar (zoals de werkmap of een portaal), kies dan daarvoor.* • *Is er géén beveiligde omgeving beschikbaar?* ➔ *Is het qua doorlooptijd mogelijk om de gegevens per post te sturen, kies dan hiervoor* ➔ *Is de enige mogelijkheid om de gegevens per e-mail te versturen, let dan op de volgende punten:* ➔ *Controleer aan wie je de mail adresseert (kijk uit voor auto aanvulling!) en maak gebruik van de BCC;* ➔ *Let er bij bijlagen op dat je het juiste bestand koppelt. Is het een bestand met veel persoonsgegevens of gevoelige gegevens, bescherm dit bestand dan met een wachtwoord wat je apart toestuurt (bijvoorbeeld per sms).* ***Deel op een manier die zo veilig mogelijk is***
	Kan je doel ook op **een andere manier** worden bereikt waarbij de privacy van de klant beter gewaarborgd wordt? *Voorbeeld: De klant schrijft zichzelf in voor een cursus in plaats van dat wij dit voor hem regelen.* ***Deel alleen persoonsgegevens als dit echt op deze manier nodig is***

Bij vragen of twijfel: werkbedrijfibp@uwv.nl
Stappenplan Veilig gegevens verwerken versie 1.0 IB&P team WERKbedrijf, 26-4-2018

Het stappenplan is op 1 mei 2018 via de nieuwsbrief aan medewerkers van het WERKbedrijf gecommuniceerd:[109]

> **07. Stappenplan 'Veilig persoonsgegevens delen' voor AVG vanaf nu beschikbaar**
>
> WET EN BELEID
>
> *Ter informatie voor: alle medewerkers*
>
> Op 25 mei 2018 dient UWV te voldoen aan de Algemene Verordening Gegevensbescherming (AVG). Daarover was eerder te lezen in de WERK in uitvoering van 10 april 2018 en de WERK in uitvoering van 24 april 2018. Deze verordening vervangt de huidige Wet bescherming Persoonsgegevens (WbP). Om je verder op weg te helpen, is vanaf nu het stappenplan 'Veilig persoonsgegevens delen' beschikbaar in de toolkit 'Algemene Verordening Gegevensbescherming (AVG)' op de Digitale Werkplek.
>
> **Waarom ook alweer de AVG?**
> De Algemene Verordening Gegevensbescherming (AVG) heeft het doel dat in alle EU-lidstaten dezelfde regels gaan gelden voor de gegevensbescherming van natuurlijke personen. De AVG dwingt organisaties om transparant te zijn over wat zij met persoonsgegevens van burgers doen. UWV werkt daar graag aan mee.
>
> **Stappenplan delen klantgegevens**
> De vuistregel om met persoonsgegevens om te gaan is: dragen de klantgegevens die je wilt delen én de ontvanger van de gegevens bij aan het uitvoeren van onze wettelijke taak? Dan is het delen ervan toegestaan. Draagt het niet bij aan de wettelijke taak? Dan is het delen van de gegevens niet toegestaan. Maar soms is de vuistregel alleen niet toereikend. Elke situatie vraagt om een afzonderlijke afweging. Om je hierbij te helpen, is het stappenplan ' Veilig persoonsgegevens delen' opgesteld. Deze is te vinden in de toolkit 'Algemene Verordening Gegevensbescherming (AVG)'. Voor meer informatie kun je eveneens terecht in deze toolkit.
>
> Meer informatie of vragen? Benader de AKI in je district.

Op de vraag of er tussen het eerste en het achtste datalek op 3 augustus 2018 technische maatregelen zijn geïmplementeerd, heeft UWV geantwoord: "*UWV heeft in die periode geen technische maatregel geïmplementeerd, maar wel meerdere organisatorische en procesmatige maatregelen doorgevoerd. We zijn echter van mening dat dit feit moet worden bezien in het licht van de risico-inschatting die UWV destijds maakte en de eerder geschetste achterstand op het gebied van IB&P maatregelen als gevolg van taakstellingen, welke wordt beschreven in de brief*".[110]

Na het achtste datalek heeft UWV op 20 augustus 2018 geanalyseerd hoe het datalek heeft kunnen plaatsvinden en hoe dit specifieke datalek richting betrokkenen is afgehandeld. Deze analyse is beschreven in een document, waarin de volgende aanbevelingen zijn opgenomen:[111]

[109] Zie dossierstukken 109 en 116 (Reactie UWV op feitelijke bevindingen, bijlage "WERK in uitvoering", punt 07).
[110] Zie dossierstukken 65 en 66 (Beantwoording door UWV, bijlage, p. 1, antwoord op vraag 1).
[111] Zie dossierstuk 38 (Excel-bestand, bijlage 42 (bestand "Microsoft Word-document" bij antwoord op vraag 18 onder datalek 7), p. 3).

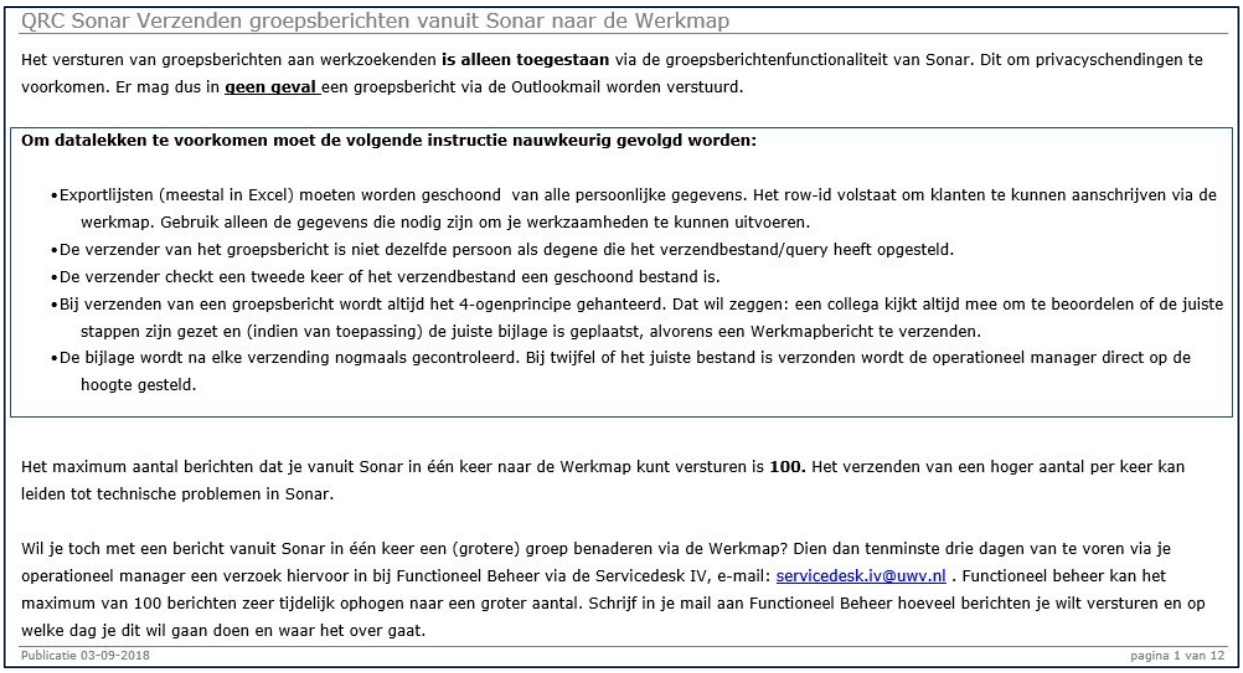
Aanbevelingen
Het incident leidt tot de volgende aanbevelingen en maatregelen ter voorkoming van dergelijke datalekken:

- Wie de query draait, selecteer alleen de strikt noodzakelijke gegevens (doelbinding).
- De verzender van de mail is niet dezelfde persoon als de querydraaier.
- De querydraaier schoont het bestand altijd op en levert alleen de strikt noodzakelijke gegevens aan degene die de zending verricht: alleen het Row-id is voor de zending nodig.
- Bij verzenden wordt altijd het 4-ogenprincipe gehanteerd: je dient de bulkmail samen met je collega te versturen.
- De bijlage van een Werkmapbericht en de verzendlijst worden onder verschillende bestandsnamen in verschillende mappen opgeborgen.
- De bijlage wordt na elke verzending nogmaals gecontroleerd. Bij twijfel of het juiste bestand is verzonden wordt de operationeel manager direct op de hoogte gesteld
- In het kader van bewustwording wordt privacy en beveiliging op de vestiging en in het district weer geagendeerd. Aan concerncommunicatie en communicatie WERKbedrijf wordt (campagnematige) ondersteuning gevraagd om privacy en beveiliging extra onder de aandacht te brengen.
- Maak het onmogelijk om Excelbestanden als bijlage bij Werkmapberichten bij te voegen. Dit betreft een technische oplossing die mogelijk in maart 2019 in productie kan worden genomen.
- Zorg dat de verzendinstructies/stappenplan geüpdatet worden en bekend zijn bij medewerkers en dat de medewerkers dit goed opvolgen. Zeker ook nieuwe medewerkers en uitzendkrachten dienen bekend gemaakt te worden met de juiste werkwijzen en instructies.
- Onderzoek of door de betrokken medewerker(s) nalatig is gehandeld en of/welke consequenties daaraan worden verbonden.

Voorts heeft UWV over de hierboven vermelde analyse aangegeven: "*Allereerst heeft WERKbedrijf in september 2018 op basis van een analyse van wat er fout ging in Alkmaar (...) - het niet volgen van de organisatorische en procesmatige beveiligingsregels- opnieuw een instructie aan medewerkers gestuurd voor de omgang met bulkberichten via de Werkmap om dit type lek te voorkomen. Meer onderzoek in de zin van een omvangrijk rapport ligt hier niet aan ten grondslag omdat de oorzaak helder was. (...) Op basis van deze analyse heeft UWV ook besloten technische maatregelen te nemen- waar men eerder vaststelde dat organisatorische en procesmatige beveiligingsmaatregelen volstonden - n.l. een blokkade in de Werkmap te bouwen waardoor er o.a. geen Excel bestanden meer mee gestuurd kunnen worden, wat medio december is gebeurd*".[112]

Op 3 september 2018, dus een maand na het achtste datalek en twee dagen voorafgaand aan het negende datalek, is de QRC groepsberichten uitgebreid met een omkaderde passage met instructies om datalekken te voorkomen:[113]

[112] Zie dossierstuk 46 (Beantwoording door UWV, bijlage 2 (bestand "Brief AP informatieverzoek 29042019"), p. 1).
[113] Zie dossierstuk 91 (Beantwoording door UWV, bijlage 4 (bestand "QRC Sonar Groepsbericht verzenden naar de Werkmap 22072013", p. 1)).



QRC Sonar Verzenden groepsberichten vanuit Sonar naar de Werkmap

Het versturen van groepsberichten aan werkzoekenden **is alleen toegestaan** via de groepsberichtenfunctionaliteit van Sonar. Dit om privacyschendingen te voorkomen. Er mag dus in **geen geval** een groepsbericht via de Outlookmail worden verstuurd.

Om datalekken te voorkomen moet de volgende instructie nauwkeurig gevolgd worden:

- Exportlijsten (meestal in Excel) moeten worden geschoond van alle persoonlijke gegevens. Het row-id volstaat om klanten te kunnen aanschrijven via de werkmap. Gebruik alleen de gegevens die nodig zijn om je werkzaamheden te kunnen uitvoeren.
- De verzender van het groepsbericht is niet dezelfde persoon als degene die het verzendbestand/query heeft opgesteld.
- De verzender checkt een tweede keer of het verzendbestand een geschoond bestand is.
- Bij verzenden van een groepsbericht wordt altijd het 4-ogenprincipe gehanteerd. Dat wil zeggen: een collega kijkt altijd mee om te beoordelen of de juiste stappen zijn gezet en (indien van toepassing) de juiste bijlage is geplaatst, alvorens een Werkmapbericht te verzenden.
- De bijlage wordt na elke verzending nogmaals gecontroleerd. Bij twijfel of het juiste bestand is verzonden wordt de operationeel manager direct op de hoogte gesteld.

Het maximum aantal berichten dat je vanuit Sonar in één keer naar de Werkmap kunt versturen is **100.** Het verzenden van een hoger aantal per keer kan leiden tot technische problemen in Sonar.

Wil je toch met een bericht vanuit Sonar in één keer een (grotere) groep benaderen via de Werkmap? Dien dan tenminste drie dagen van te voren via je operationeel manager een verzoek hiervoor in bij Functioneel Beheer via de Servicedesk IV, e-mail: servicedesk.iv@uwv.nl . Functioneel beheer kan het maximum van 100 berichten zeer tijdelijk ophogen naar een groter aantal. Schrijf in je mail aan Functioneel Beheer hoeveel berichten je wilt versturen en op welke dag je dit wil gaan doen en waar het over gaat.

Publicatie 03-09-2018 pagina 1 van 12

Bij het eerste punt in de hierboven genoemde passage uit QRC groepsberichten van 3 september 2018 staat dat de exportlijsten voor het verzenden van groepsberichten eerst door de medewerkers dienen te worden geschoond door het verwijderen van gegevens uit het bestand. Daardoor blijft alleen het row-ID over. Verder staat er in deze versie van de QRC groepsberichten dat het 4-ogenprincipe gehanteerd moet worden. In eerdere versies van de verstrekte QRC groepsberichten waren deze instructies over het schonen en het row-ID en het 4-ogenprincipe niet opgenomen.

Op 4 september 2018 heeft de AP een telefonisch overleg gehad met de FG van UWV. Daarin is onder andere stilgestaan bij de vraag of er inmiddels technische maatregelen waren ingevoerd. In dat gesprek heeft de FG aangegeven dat er, voor zover bij hem bekend, op dat moment nog geen technische maatregelen waren ingevoerd. Hij gaf verder aan dat het vier-ogenprincipe wel was ingevoerd. Hij vond dat de werkwijze inherent onveilig is nu er gegevens uit een systeem worden onttrokken en in een kantoorapplicatie verder worden verwerkt. Hij was van mening dat medewerkers van UWV met een systeem moeten werken dat onvoldoende waarborgen heeft.[114]

De FG van UWV heeft naar aanleiding van het achtste datalek op verzoek van de Raad van Bestuur van UWV onderzoek gedaan en heeft dit beschreven in de "*FG rapportage van bevindingen: Datalek Alkmaar*" van 30 november 2018.[115] De resultaten van dat onderzoek heeft de FG op 22 januari 2019 aan de Raad van Bestuur en directie Werkbedrijf gepresenteerd.[116] In die presentatie is onder meer opgenomen:

[114] Zie dossierstuk 22 (Telefoonnotitie FG UWV).
[115] Zie dossierstuk 81, bijlage 5 (bestand "Vraag 16_Concept FG -rapportage") en dossierstukken 109 en 116 (Reactie UWV op feitelijke bevindingen, p. 3).
[116] Zie dossierstuk 38 (Excel-bestand, antwoord op vraag 11 onder datalek 7) en dossierstuk 51 (bestand "Resultaten FG-onderzoek Werkbedrijf v010", p. 7 en 9).

"*Maatregel om de upload van Excel-bestanden naar de werkmap onmogelijk te maken werkt voor dit specifieke lek. (…)*
"*Pleisters Plakken: Procesafspraken zijn niet 'hard' afgedwongen*" (…)
"Beleid komt niet aan op de Werkvloer:

- *Begrijpen van procesafspaken*
- *Awereness bereikt niet alle medewerkers"*

Uiteindelijk heeft UWV medio december 2018 een technische maatregel ingevoerd, namelijk het blokkeren van de mogelijkheid tot het toevoegen van onder andere Excel-bestanden bij het verzenden van groepsberichten via de Mijn werkmap-omgeving.[117]

UWV heeft met betrekking tot de vraag hoe is gecontroleerd of maatregelen ook daadwerkelijk zijn ingevoerd geantwoord dat UWV en WERKbedrijf niet als zodanig hebben gecontroleerd of maatregelen die zijn genomen naar aanleiding van datalekken daadwerkelijk zijn ingevoerd.[118]

Op de vraag of UWV externe partijen onderzoek had laten doen naar aanleiding van de datalekken, antwoordt UWV met betrekking tot de eerste acht datalekken: "*UWV zag op dat moment geen toegevoegde waarde in het laten uitvoeren van een extern onderzoek omdat gezien de genomen maatregelen, het risico gemitigeerd leek*".[119] UWV heeft ten aanzien van het achtste datalek wel gesteld: "*UWV Intern onderzoek door Bestuurszaken in opdracht van FG waarbij extern expertise is ingewonnen van een consultant*".[120]

UWV stelt ten aanzien van de wijze waarop zij evaluaties uitvoert het volgende: "*Er is geen formeel geprotocolleerd evaluatieproces doorlopen na ieder van de zeven datalekken. Dat is niet de manier waarop UWV in alle gevallen werkt. Betrokken afdelingen concludeerden gedurende geruime tijd in goed overleg dat de in 2016 genomen maatregelen volstonden. Deze conclusie bleek achteraf helaas onjuist*".[121] UWV vermeldt als reactie op de feitelijke bevindingen echter dat er wel evaluaties zijn uitgevoerd met betrekking tot genomen maatregelen.[122] Deze stelling dat er wel geëvalueerd zou zijn wordt niet onderbouwd met documentatie waaruit de evaluatie daadwerkelijk blijkt.

[117] Zie dossierstuk 38 (Beantwoording door UWV, brief), dossierstuk 38 (Excel-bestand, antwoord op vraag 13 onder datalek 6 en 7), dossierstukken 65 en 66 (Beantwoording door UWV, p. 2 en bijlage, p. 1, antwoord op vraag 2) en dossierstuk 81 (Beantwoording door UWV, bijlage 1 (bestand "Beantwoording vragen AP augustus 2019", antwoord op vraag 17)).
[118] Zie o.a. dossierstuk 38 (Excel-bestand, antwoord op vraag 17 onder datalek 1 t/m 7).
[119] Zie dossierstuk 38 (Excel-bestand, antwoord op vraag 12 onder datalek 1 t/m 6).
[120] Zie dossierstuk 38 (Excel-bestand, antwoord op vraag 12 onder datalek 7).
[121]Zie dossierstukken 65 en 66 (Beantwoording door UWV, bijlage, p. 2, antwoord op vraag 5).
[122] Zie dossierstukken 109 en 116 (Reactie UWV op feitelijke bevindingen, p. 3).