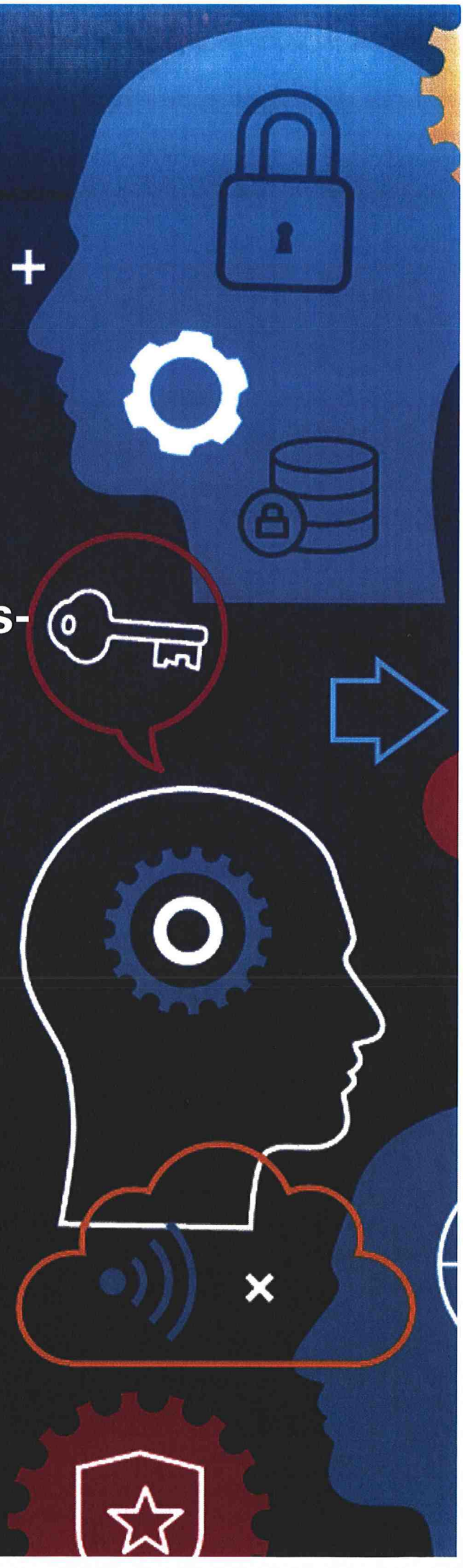
KPMG

Uitvoeringsinstituut
Werknemersverzekeringen

[redacted]

Privacy & informatiebeveiligings-onderzoek SONAR



12 augustus 2020

A1900018081

KPMG Advisory N.V.

Leverancier ID: 0000002802

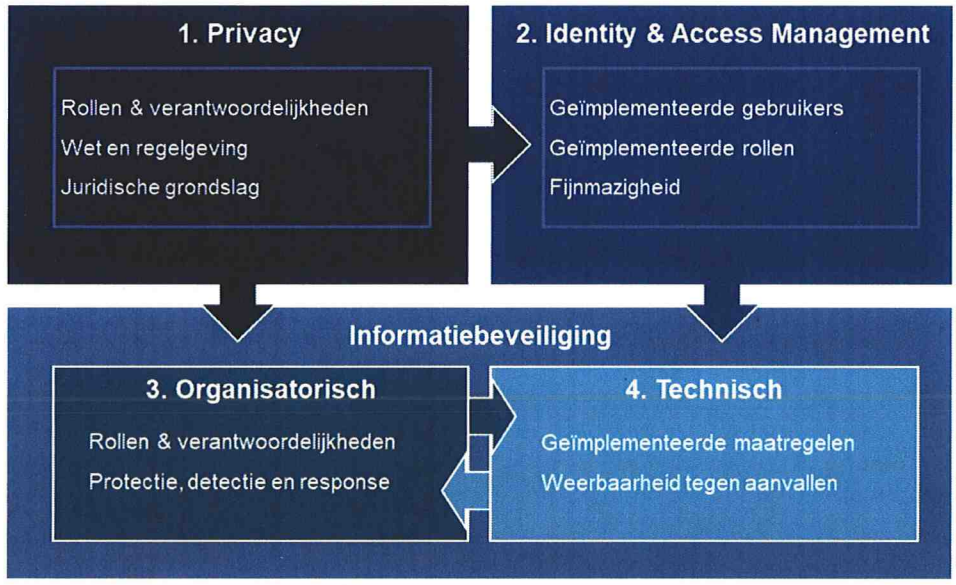
Inhoudsopgave

1 Managementsamenvatting

De kernactiviteiten van UWV-divisie WERKbedrijf bestaan uit arbeidsbemiddeling en re-integratie. SONAR is een van de hoofdapplicaties ter ondersteuning van deze kernactiviteiten en telt circa zestienduizend actieve gebruikers. Naast het WERKbedrijf maken andere divisies (Uitkeren, Handhaving, Bezwaar en Beroep, en Sociaal Medische Zaken) en ketenpartners veelvuldig gebruik van SONAR. In de SONAR applicatie worden noodzakelijkerwijs veel (gevoelige en soms bijzondere) persoonsgegevens van burgers verwerkt. Het is daarom van belang dat deze persoonsgegevens zorgvuldig worden verwerkt.

1.1 Het onderzoek dat wij hebben uitgevoerd

U heeft KPMG Cyber (hierna: KPMG) gevraagd een onderzoek te doen naar de huidige stand van de getroffen maatregelen voor de zorgvuldige verwerking van deze persoonsgegevens. Daarvoor hebt u een lijst van onderzoeksvragen opgesteld om met de antwoorden en aanvullend advies de grootste risico's te kunnen beheersen. Om goed antwoord op de vragen te geven en u van constructief advies te kunnen voorzien, hebben wij volwassenheidsmetingen uitgevoerd in de domeinen (1) Privacy, (2) Identity & Access Management en Informatiebeveiliging ((3) Organisatorisch en (4) Technisch) welke nauw met elkaar verbonden zijn, zoals onderstaand weergegeven:



Elk van deze domeinen is separaat onderzocht. Hierover hebben wij gerapporteerd in de vorm van een rapportage per deelonderzoek:

1. Deelonderzoek Privacy (d.d. 14 juli 2020, 50 bladzijden);
2. Deelonderzoek Identity and Access Management (d.d. 14 juli 2020, 48 bladzijden);
3. Deelonderzoek Informatiebeveiliging (organisatorisch) (d.d. 14 juli 2020, 33 bladzijden)
4. Deelonderzoek Informatiebeveiliging (technisch) (d.d. 14 juli 2020, 69 bladzijden)

De rapportages per deelonderzoek vormen de bijlages bij deze rapportage, maar zijn integraal onderdeel van deze rapportage en het onderzoek.

Het voorliggende rapport, vormt de overkoepelende rapportage welke de inzichten van de verschillende domeinen samenbrengt tot een geheel. Dit rapport dient dan ook gelezen te worden in de context van de deelonderzoeken en vice versa.

1.2 Resultaten van ons onderzoek

Gezien het risicoprofiel van de gegevens die in SONAR worden verwerkt (bijzondere / gevoelige (geen financiële) persoonsgegevens) verwachten wij dat de volwassenheid van de verschillende domeinen in bovenstaande model op een schaal van 1 – 5[1] tenminste tussen 3 (Gedefinieerd) en 4 (Gemanaged) zou liggen. Op dat niveau is er sprake is van een duidelijk gedefinieerd en vastgelegd proces voor toegangsbeheer met maatregelen die passend zijn voor de gevoeligheid van de gegevens, waarbij het proces kan worden gemonitord en op basis daarvan kan worden bijgesteld. Afhankelijk van de risicobereidheid van de organisatie kan overwogen worden om (op onderwerpen) een hoger volwassenheidsniveau te ambiëren.

Echter, op basis van ons onderzoek hebben wij vastgesteld dat de volwassenheid zich bevindt tussen niveau 1 (Initieel) en 2 (Herhaalbaar) op de diverse onderdelen van het model en daarmee ook voor het totale model. Dit niveau is gezien de gevoeligheid van de gegevens in SONAR te laag. Dit lage niveau komt dan ook tot uitdrukking in de beantwoording van de vragen: vrijwel alle gestelde vragen hebben wij negatief moeten beantwoorden.

Op basis van ons onderzoek stellen wij vast dat SONAR op dit moment niet voldoet aan de privacy-beginselen toegang, rechtmatigheid, dataminimalisatie, doelbinding en opslagbeperking en daarmee niet voldoet aan de eisen vanuit de AVG. Primair is het ontbreken van een voldoende volwassenheid op de diverse deelgebieden een risico voor de voormalige, huidige en toekomstige klanten[2] van het UWV WERKbedrijf. Hun (historische) gegevens kunnen worden ingezien door een disproportionele groep medewerkers van het UWV WERKbedrijf. Daarmee is de privacy van UWV WERKbedrijf's klanten onvoldoende gewaarborgd. Secundair kan het niet voldoen aan de AVG voor het UWV WERKbedrijf leiden tot boetes, met eventuele maatschappelijke onrust en politieke impact als gevolg.

1.3 Kwantitatief overzicht van onze detailbevindingen

In onderstaande tabel zijn de bevindingen per domein kwantitatief weergeven op basis van het door ons ingeschatte risiconiveau:

	Aantal bevindingen per deelonderzoek inclusief totalen			
Deelonderzoek / risiconiveau	**Hoog**	**Midden**	**Laag**	**Totaal**
Privacy	25	7	1	**33**
Identity & Access Management	9	7	1	**17**
Informatiebeveiliging Organisatorisch	7	8	1	**16**
Informatiebeveiliging Technisch	8	3	-	**11**
Totaal	**49**	**25**	**3**	**77**

Alle bevindingen zijn afgestemd met zowel de betreffende functionarissen van UWV WERKbedrijf als het management team van het WERKbedrijf, welke alle bevindingen heeft geaccepteerd.

[1] 1 - Initieel, 2 – Herhaalbaar, 3 – Gedefinieerd, 4 – Gemanaged en 5 – Geoptimaliseerd

[2] Met klanten wordt bedoeld: alle burgers die in SONAR zijn opgenomen.

1.4 Belangrijkste oorzaken en aanbevelingen

De belangrijkste twee oorzaken die ten grondslag liggen aan het feit dat de privacy van klanten van het UWV WERKbedrijf niet voldoende gewaarborgd is (zie 1.2), zijn:

1. UWV WERKbedrijf heeft weliswaar inzicht in de koppeling tussen de bedrijfsmatige functie van haar medewerkers, en de tabbladen die zij kunnen benaderen. Echter, er is geen actueel en volledig inzicht in de koppeling tussen tabbladen en de persoonsgegevens die hierbinnen benaderd kunnen worden. In het project Autorisatie Segmentering Gemeenten (ASG) is voor de gemeente-gebruikers wel een aanzet gedaan om dit in kaart te brengen, maar dit is niet volledig en actueel, en betreft daarnaast slechts een klein percentage van het totaal aantal gebruikers. Het gebrek aan inzicht en bewuste keuzes met betrekking tot de koppeling van bedrijfsmatige functie naar de persoonsgegevens die benaderd kunnen worden hebben ertoe geleid dat vrijwel alle gebruikers (WERKbedrijf, divisies, gemeenten, etc) in de praktijk toegang tot vrijwel alle persoonsgegevens van klanten van het UWV WERKbedrijf, zonder dat daar in veel gevallen een aantoonbare noodzaak voor is.

   Wij adviseren om de koppeling tussen de bedrijfsmatige functie van de gebruikers en de persoonsgegevens die zij nodig hebben, in kaart te brengen. Met deze informatie dient de SONAR configuratie zodanig te worden aangepast dat er een duidelijke koppeling tussen bedrijfsmatige functie en benodigde persoonsgegevens is. De vastlegging van de noodzaak van de informatie per gebruiker, vormt de benodigde input voor het voldoen aan toegang, rechtmatigheid, dataminimalisatie en doelbinding. Daarmee kan ook worden gerechtvaardigd dat een selectie van medewerkers landelijk toegang heeft tot de gegevens van alle klanten in SONAR (voor de uitvoering van hun wettelijke taak). Hiermee wordt gelijk aan deze aspecten van de AVG voldaan. Periodieke controles op het naleven van dit model zorgen voor het blijvend voldoen aan de AVG.

   Het in kaart brengen van deze koppeling is een complexe activiteit gegeven de vele functierollen (meer dan 100), veelvoud aan verschillende datavelden en verspreiding van de medewerkers over divisies en locaties. Dit is dan ook niet te onderschatten, doch noodzakelijk. Ongeacht welke oplossing UWV WERKbedrijf nu in gebruik heeft (in de vorm van SONAR) of in de toekomst naartoe migreert (WorkIT); de toegang van personen tot data moet onder controle zijn.

2. De informatiebeveiligingsmaatregelen zijn op papier voor het merendeel aanwezig, maar worden in de praktijk niet (volledig en/of correct) geïmplementeerd. Periodieke controle op de implementatie ontbreekt, waardoor UWV WERKbedrijf niet in control is van de informatiebeveiligingsrisico's. Zo bevatten zowel de SONAR applicatie als het ondersteunende landschap significante kwetsbaarheden. Deze kwetsbaarheden stellen een aanvaller in staat volledige toegang (lezen, schrijven, verwijderen) te verkrijgen tot SONAR en alle gevoelige (persoons)gegevens vanaf het interne netwerk van UWV.

   Wij adviseren aan de significante kwetsbaarheden het SONAR landschap te mitigeren of compenseren. Dit borgt de privacy-beginselen rechtmatigheid, dataminimalisatie, doelbinding en opslagbeperking.

   Ook adviseren wij de effectiviteit van de implementatie van de controlemaatregelen periodiek te controleren om zodoende helder zicht te houden op de effectiviteit van de maatregelen en bij te kunnen sturen wanneer nodig. Daarmee wordt geborgd dat het UWV WERKbedrijf wanneer zij eenmaal voldoen aan de privacybeginselen – en daarmee aan de AVG, dat ook kunnen vasthouden.

Voor meer details verwijzen wij u naar de verschillende deelonderzoeken die als bijlagen bij dit rapport zijn gevoegd met daarin een beschrijving van de aanpak en de (detail)resultaten van de verschillende deelonderzoeken.

1.5 Indicatoren van achterliggende oorzaken

De ervaring leert dat kwetsbaarheden in processen en techniek in de praktijk vaak voortkomen uit onderliggende oorzaken op een hoger niveau (bijv. governance en/of cultuur). We hebben indicaties voor dergelijke onderliggende oorzaken waargenomen.

UWV is een grote en complexe organisatie. Inherent hier aan is dat bij de beheersing van de SONAR-omgeving veel verschillende (ook externe) partijen betrokken zijn, hetgeen een sterke wisselwerking veroorzaakt tussen UWV centraal en decentrale divisies. Binnen elk van de betrokken partijen zijn de verantwoordelijkheden voor onderdelen van SONAR (privacy, toegangsbeheer, beveiliging) weer verder verdeeld over verschillende teams en personen. Om voor ons onderzoek vervolgens een goed beeld van de situatie te krijgen, hebben we veel verschillende personen gesproken, die soms van elkaar niet wisten hoe de verdeling van kennis en verantwoordelijkheden nu precies is ingeregeld. Goede sturing en monitoring van de uitgezette acties is daardoor cruciaal.

De complexiteit en grootte van UWV betekent ook dat een adequate monitoring en controle op naleving van het beleid van groot belang zijn. Wij hebben op basis van ons onderzoek vastgesteld dat dit nu nog niet op het gewenste niveau is. Op basis van het opgestelde heeft het IV-bestuur WERKbedrijf verwachtingen ten aanzien van de implementatie in de praktijk. Echter, die verwachtingen komen niet overeen met wat wij in de praktijk hebben vastgesteld. Wanneer actieve monitoring en controle op de naleving van het beleid effectief zouden zijn geïmplementeerd, had WERKBedrijf dit verschil zelf al kunnen constateren. Wij adviseren om de samenwerking tussen centraal en decentraal verder te verstevigen om deze monitoring en controle effectiever in te richten.

Wij adviseren UWV WERKbedrijf de genoemde oorzaken van onduidelijke toewijzing van verantwoordelijkheden en inadequate monitoring en controle op de naleving nader te onderzoeken, zodat verbeteringen ook op de lange termijn standhouden.

We begrijpen dat zowel de belangrijkste oorzaken als de indicatoren van achterliggende oorzaken in een veel bredere context dan alleen WERKBedrijf spelen. Wij adviseren dan ook om naast het perspectief van het WERKBedrijf, ook vanuit een UWV-breed perspectief de in onze rapportages geïdentificeerde problematiek nader te onderzoeken en aan te pakken. Dit UWV-breed perspectief is randvoorwaardelijk voor het realiseren van de structurele verbeteringen op de toegang tot de klantgegevens en op de beveiliging van die gegevens tegen ongeautoriseerde toegang.

Wij hebben begrepen dat de SONAR omgeving op termijn wordt vervangen. Dit betekent dat een afweging moet worden gemaakt of de verbeteringen die wij in deze en onderliggende rapportages hebben geïdentificeerd nog kunnen worden opgelost in de huidige SONAR omgeving of in de vervangende applicatie. Wij adviseren u om hiervoor een analyse te maken en daarbij de huidige risico's af te wegen tegen de kosten voor het oplossen van deze risico's in de huidige SONAR omgeving en daarin de doorlooptijd van vervanging van SONAR, de belangrijke rol van SONAR voor het primaire proces van UWV WERKbedrijf en het maatschappelijk belang van adequate privacy en securitymaatregelen hierin goed mee te wegen. Het is naar onze mening dan ook noodzakelijk dat tenminste een (deel) oplossing op korte termijn wordt gevonden voor de grootste risico's en daarmee niet te wachten tot de implementatie van de vervangende omgeving op de langere termijn.

1.6 Bestuurlijke reactie UWV WERKbedrijf

Op basis van de voornoemde resultaten hebben wij de volgende bestuurlijke reactie ontvangen van UWV WERKbedrijf:

"De directie van UWV WERKbedrijf neemt de bevindingen die in het rapport staan opgesomd uitermate serieus. De maatregelen die WERKbedrijf reeds gerealiseerd had, zoals de Excelblokkade in de werkmap, dataminimalisatie in de dashboards en het aanscherpen van autorisatieprofielen voor gemeenten, zijn nog niet voldoende. Daarom zal WERKbedrijf met spoed aanvullende maatregelen nemen om de risico's verder te mitigeren. WERKbedrijf zal, naast het per direct versnellen van de reeds geplande maatregelen, de bevindingen en voorgestelde maatregelen van KPMG projectmatig op gaan pakken. De stuurgroep die dit project zal aansturen, zal op directieniveau georganiseerd worden."

1.7 Afsluiting

Graag wijzen wij u er op dat dit onderzoek niet gericht op het uitvoeren van een accountantscontrole, beoordelingsopdracht of andere assuranceopdracht. Er kan derhalve geen zekerheid worden verstrekt over de getrouwheid van financiële of andere informatie. Daarnaast blijft UWV WERKbedrijf te allen tijde verantwoordelijk voor:

- de opzet en werking van de maatregelen van interne beheersing van de organisatie;
- de bestuurlijke besluitvorming die betrekking heeft op het ontwerp- en implementatieproces van het informatiesysteem in de financiële keten;
- de werking van systemen inclusief de door deze systemen gebruikte of gegenereerde gegevens.

Deze rapportage is uitsluitend bedoeld voor het UWV WERKbedrijf als zijnde onze opdrachtgever. Zonder onze uitdrukkelijke en voorafgaande schriftelijke toestemming is het niet toegestaan deze rapportage, dan wel delen van deze rapportage, te gebruiken voor andere doeleinden, openbaar te maken en/of aan derden te verstrekken. Wij aanvaarden geen aansprakelijkheid voor het gebruik van deze rapportage anders dan waarvoor deze is opgesteld en aan het UWV WERKbedrijf als opdrachtgever beschikbaar is gesteld.

Wij hopen u met deze rapportage voldoende te hebben geïnformeerd en zijn vanzelfsprekend bereid om deze rapportage nader toe te lichten.

Hoogachtend,

KPMG Advisory N.V.