Uitvoeringsinstituut
Werknemersverzekeringen

VERTROUWELIJK

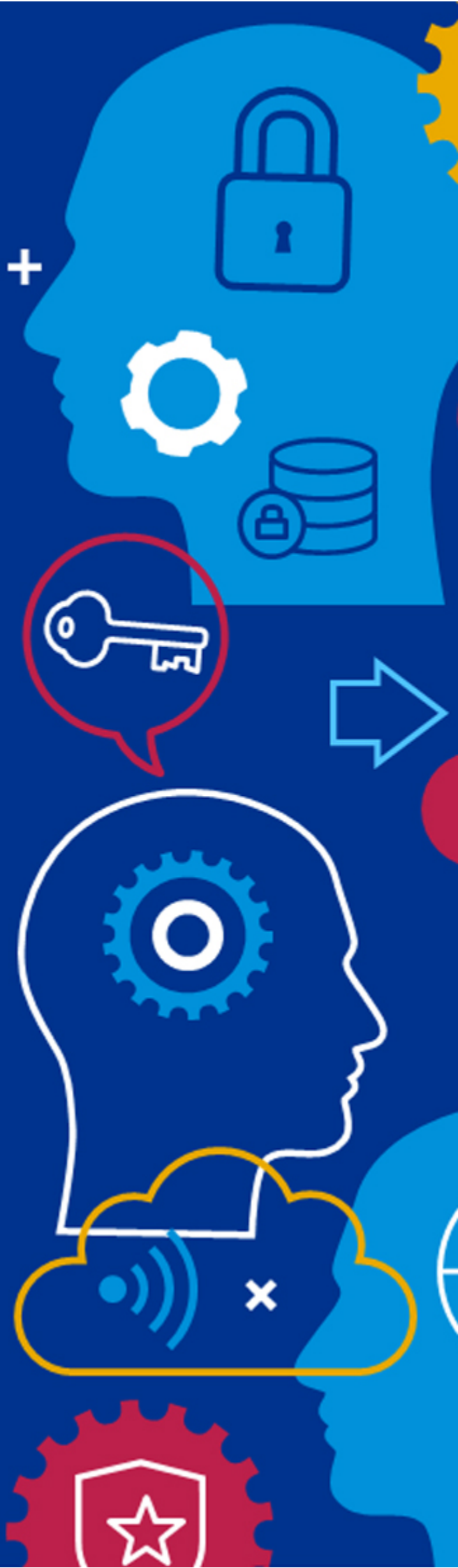
Deelonderzoek 1: Privacy – SONAR

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 één van de hoofdapplicaties ter ondersteuning van deze kernactiviteiten en telt circa zestienduizend actieve gebruikers. Naast het UWV 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[1]. Het is daarom belangrijk dat SONAR voldoet aan privacywet- en regelgeving, met name de Algemene Verordening gegevensbescherming (hierna: AVG). UWV WERKbedrijf heeft KPMG Advisory N.V. (hierna: 'KPMG') daarom gevraagd een aantal specifieke privacyvragen met betrekking tot SONAR te beantwoorden en daarnaast een breder Privacy & informatiebeveiligingsonderzoek naar SONAR uit te voeren. Het totale onderzoek valt uiteen in vier deelonderzoeken: Privacy, Identity & Access Management, Informatiebeveiliging: technisch en Informatiebeveiliging: organisatorisch. Voor u ligt het resultaat van het deelonderzoek Privacy. Het doel van dit deelonderzoek is het vaststellen van de privacy volwassenheid, waarbij een aantal specifieke vragen van UWV WERKbedrijf zijn meegenomen.

Hieronder is een samenvatting gegeven van de belangrijkste bevindingen en observaties die geïdentificeerd zijn gedurende dit onderzoek, alsmede onze belangrijkste aanbevelingen voor opvolging.

SONAR voldoet niet aan de vereisten van de AVG

SONAR voldoet momenteel aan geen van de beginselen uit de AVG (die onderliggend zijn aan de door UWV WERKbedrijf opgestelde privacy vragen ten behoeve van dit onderzoek) op het gebied van rechtmatigheid, minimale gegevensverwerking, doelbinding, opslagbeperking en het waarborgen van de integriteit en vertrouwelijkheid.

Rechtmatigheid

[redacted] Art. 10 lid 2 sub e en g Wob

Daarnaast vindt geen controle op doelbinding van vrije invoervelden plaats. Hierdoor is deze gegevensverwerking niet rechtmatig.

Minimale gegevensverwerking

Niet alle eindgebruikers van SONAR die toegang hebben tot klantgegevens, hebben dit ook daadwerkelijk nodig voor de uitoefening van hun functie. Daarnaast wordt SONAR als archiveringssysteem gebruikt. Als gevolg daarvan bevat SONAR een zeer groot aantal persoonsgegevens van zowel actieve als inactieve klanten, die te raadplegen en te exporteren zijn door de gebruikers. SONAR bevat persoonsgegevens van tenminste 3,1 miljoen inactieve klanten.

Doelbinding

De applicatie SONAR kent ca. 15.000 gebruikers die nagenoeg allemaal inzage hebben in alle persoonsgegevens van alle klanten die in SONAR zijn opgenomen. Deze gebruikers bestaan uit verschillende gebruikersgroepen, die persoonsgegevens in SONAR voor uiteenlopende doeleinden verwerken. Niet iedere gebruiker heeft toegang nodig tot alle persoonsgegevens in SONAR om zijn werkzaamheden te kunnen uitvoeren. Denk aan het verschil tussen een administratief medewerker en een manager, maar ook het verschil

[1] De definitie van 'gevoelig persoonsgegeven' wordt niet limitatief opgesomd in de AVG, maar o.a. in préambule 75 AVG, en art. 46 UAVG wordt nadere invulling van het begrip gegeven. Zij verder B5.2 van dit rapport over de invulling hiervan.

tussen het UWV WERKbedrijf van UWV en andere divisies. Er wordt in het autorisatiemodel te beperkt onderscheid gemaakt op basis van het 'need-to-have'-principe, bijvoorbeeld op basis van regio, partij (intern of extern), gegevensvelden, klanten, of tabbladen, hetgeen niet in verhouding staat tot het doel.

Opslagbeperking

Persoonsgegevens in SONAR worden niet of in beperkte mate geschoond (de laatste schoningsactie ten tijde van ons onderzoek was in 2018, wij zijn geïnformeerd dat in 2020 ook een schoningsactie heeft plaatsgevonden), ook niet na het verstrijken van de wettelijke bewaartermijn. Als gevolg daarvan ontbreekt de wettelijke grondslag voor het verwerken van persoonsgegevens na het verstrijken van de bewaartermijn. Daarnaast blijven klanten voor alle gebruikers zichtbaar, terwijl dit niet noodzakelijk is en doelbinding ontbreekt.

[redacted].[2] [redacted]

Art. 10 lid 2 sub e en g Wob

Ook de bredere analyse aan de hand van ons privacy-raamwerk laat zien dat SONAR niet voldoet aan de vereisten van de AVG. De privacy-volwassenheid is lager dan verwacht mag worden van een applicatie die naar de aard, context, hoeveelheid en gevoeligheid van de verwerkingen een inherent hoog privacyrisico kent. SONAR bevat namelijk veel (bijzondere) persoonsgegevens van miljoenen klanten, zoals van werkzoekenden, (gedeeltelijk) arbeidsongeschikten, kinderen, Wajong'ers en bijstandsgerechtigden.

[redacted]

Art. 11 lid 1 Wob

Doordat de gegevensverwerking in SONAR niet voldoet aan de beginselen vanuit de AVG, loopt UWV het risico op datalekken en handhavend optreden door de Autoriteit Persoonsgegevens (AP). Ook kan de AP als ultimum remedium een verwerkingsverbod opleggen, wat betekent dat persoonsgegevens in SONAR niet meer verwerkt mogen worden.

Directe actie is daarom vereist

Het belangrijkste risico ten aanzien van de gegevensverwerking in SONAR is dat de ca. 15.000 eindgebruikers alle persoonsgegevens van miljoenen klanten van UWV WERKbedrijf kunnen inzien en exporteren. Het inperken van deze rechten (zowel het aantal eindgebruikers als de mate van inzage in persoonsgegevens) is de belangrijkste maatregel die UWV WERKbedrijf op zo kort mogelijke termijn moet nemen. Wij hebben echter

[2] [redacted] Art. 10 lid 2 sub e en g Wob

begrepen dat SONAR een legacy-systeem is hetgeen implementatie van deze maatregel in de weg staat. Het deelonderzoek Identity & Access Management gaat hier nader op in.

Gezien het belang van de SONAR applicatie voor het primaire proces van UWV WERKbedrijf en de legacy-problematiek van deze applicatie, zal SONAR actief moeten blijven totdat voldoende maatregelen zijn genomen om de risico te beperken of een vervangend systeem beschikbaar is. Hieronder hebben wij enkele korte termijn acties geïdentificeerd, waar geen substantiële verandering in de architectuur van SONAR mee gemoeid is. Deze korte termijn acties mitigeren slechts beperkt de belangrijkste risico's. Deze gaan uit van een korte overbruggingsperiode naar de geplande vervanging van SONAR, waarbij rekening houdend met de lengte van die overbruggingsperiode in verhouding tot het risiconiveau, de risico's tot een acceptabel, tijdgebonden restrisico dienen te worden teruggebracht. Het is van belang om de afweging van deze risico's te documenteren zodat UWV WERKbedrijf aan de toezichthouder kan aantonen dat het in controle is.

Om de risico's ten aanzien van de verwerking van persoonsgegevens in SONAR te verkleinen raden wij aan om de hieronder genoemde acties op korte termijn te implementeren. Bij het definiëren van deze acties hebben wij rekening gehouden met de (technische) capaciteit van SONAR om deze verbeteringen door te voeren. Deze acties beperken echter maar een gedeelte van de privacy-risico's. Er is een structurele verbeteringsslag op SONAR of een vervangend systeem nodig om alle risico's te mitigeren. Voor alle gedetailleerde bevindingen en aanbevelingen verwijzen wij naar Appendix A.

Korte termijn acties om de privacy-risico's te verkleinen

— Implementeer een periodiek opschoningsproces dat minimaal jaarlijks onnodige data verwijdert.

— Maskeer de persoonsgegevens van inactieve klanten uit SONAR conform de wijze waarop persoonsgegevens van overledenen worden gemaskeerd, zodat deze niet meer zichtbaar zijn voor eindgebruikers.

— [redacted] Art. 10 lid 2 sub e en g Wob

— Zorg dat de toegan-gsrechten voor planbureaus en soortgelijke afdelingen opgeschoond worden, zodat zij geen toegang meer hebben tot SONAR, wanneer eAfspraak in WorkIT is geïmplementeerd.

— Zorg voor een hogere privacy awareness bij gebruikers. Besteed in de awareness-trainingen extra aandacht aan het risico van datalekken, vrije invoervelden en het veilig gebruiken en verwijderen van geëxporteerde SONAR-gegevens. Controleer tevens regelmatig op de naleving en effectiviteit van de nieuwe gedragsregels.

— Zorg ervoor dat het privacy statement op werk.nl adequaat de (belangrijkste) verwerkingen en ten minste alle bijzondere persoonsgegevens weergeeft, om te voldoen aan het transparantiebeginsel,

Structurele verbeteringen

— Beperk de inzagerechten, bijvoorbeeld op basis van functie medewerker of ketenpartner, regio, soort dienstverlening en/of type klant. Het deelonderzoek Identity & Access Management gaat hier nader op in.

— Zorg dat de applicatie de dagelijkse bedrijfsprocessen zodanig functioneel kan ondersteunen, dat de exportmogelijkheid voor de standaardgebruiker uitgezet kan worden.

— Hoewel privacy een verantwoordelijkheid van de gehele lijn is, wordt eigenaarschap hiervan niet door de hele organisatie van het UWV WERKbedrijf genomen. Zorg voor een privacynetwerk van 'privacy

champions' in de regiokantoren, toegewijde privacy resourcing en KPI's in het applicatiebeheerteam, en bewuste privacy-risicoafwegingen van het management.

— [redacted] Art. 10 lid 2 sub e en g Wob

— Breng de klantgegevens van inactieve klanten (gestructureerde data) over naar een archiveringssysteem zodat de 3,1 miljoen inactieve klanten niet zichtbaar zijn voor de 15.000 gebruikers als deze niet nodig zijn voor het dagelijkse werk.

— Creëer een compleet en gedetailleerd overzicht van alle categorieën persoonsgegevens in SONAR, en welke afdelingen en ketenpartners welke categorieën nodig hebben voor welke doeleinden.

De ervaring leert dat privacykwetsbaarheden vaak voortkomen uit onderliggende oorzaken op een hoger niveau (bijv. op procesniveau, bestuursniveau en cultuur/mensen). We hebben indicaties voor dergelijke onderliggende oorzaken waargenomen. Daarom is het advies onderstaande grondoorzaken nader te onderzoeken, zodat verbeteringen ook op de lange termijn standhouden.

Veel privacyrisico's van SONAR zijn in de afgelopen twee jaar al aangekaart door het UWV-brede Bureau Gegevensbescherming, de afdeling Informatiebeveiliging & Privacy van het WERKBedrijf en de Autoriteit Persoonsgegevens. Deze zijn echter beperkt gemitigeerd. Wij hebben tijdens ons onderzoek begrepen dat een discussie hierover vaak strandt door de onderstaande twee factoren.

Onderhoudsproblematiek SONAR

SONAR kent een onderhoudsproblematiek die implementatie en aanpassing van maatregelen in de applicatie in de weg staat. SONAR is een legacy-systeem dat niet gebouwd is met de principes van privacy-by-design en privacy-by-default, zoals pseudonimisering en het beginsel van minimale gegevensverwerking, aangezien de AVG toen nog niet van kracht was. SONAR bestaat uit ca. 50% maatwerk, is weinig flexibel, en releases hebben een doorlooptijd van vele maanden. Dat veroorzaakt problemen bij het realiseren van nieuwe gebruikerswensen of richtlijnen. Voorgenomen wijzigingen op het gebied van privacy raken regelmatig ondergesneeuwd door urgentere issues ten behoeve van de operationele processen.

Te ruime interpretatie van de wet SUWI

De wet SUWI geeft een grondslag voor (regionale) samenwerking tussen UWV en gemeentes. Deze wettelijke grondslag voor samenwerking is vaak gebruikt als reden om de ruime inzagerechten niet aan te passen. Belangrijk is hierbij dat voldoen aan de AVG en samenwerking tussen ketenpartners hand in hand kunnen gaan. Artikel 76 SUWI beschrijft dat het UWV zorg moet dragen voor "de nodige technische en organisatorische voorzieningen ter beveiliging van hun gegevens tegen verlies of aantasting en tegen onbevoegde kennisneming, wijziging en verstrekking van die gegevens". Hier mag onder andere onder verstaan worden dat toegang tot de gegevens in SONAR op basis van het 'need-to-have' principe plaats moet vinden.

2 Inleiding

2.1 Achtergrond

De kernactiviteiten van UWV-divisie UWV 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 UWV WERKbedrijf maken andere divisies (Handhaving, Bezwaar en Beroep, en Sociaal Medische Zaken) en ketenpartners veelvuldig gebruik van SONAR. In de SONAR-applicatie worden noodzakelijkerwijs veel (gevoelige) persoonsgegevens van burgers verwerkt. Het is daarom belangrijk dat SONAR passende technische en organisatorische maatregelen ten behoeve van toegangsbeheer (Identity & Access Management, kortweg IAM) heeft ingericht. UWV WERKbedrijf heeft KPMG Advisory N.V. (hierna: 'KPMG') gevraagd een onderzoek uit te voeren naar de volwassenheid van het toegangsbeheer in SONAR, en daarin een aantal specifieke privacyvragen met betrekking tot SONAR mee te nemen. Het totale onderzoek valt uiteen in vier deelonderzoeken: Privacy, Identity & Access Management, Informatiebeveiliging: technisch en Informatiebeveiliging: organisatorisch. Voor u ligt het resultaat van het deelonderzoek Privacy.

2.2 Doelstelling

Het doel van dit deelonderzoek is het vaststellen van de volwassenheid van toegangsbeheer rondom SONAR, waarbij een aantal selectie van privacyvragen van UWV WERKbedrijf zijn meegenomen.

#	UWV specifieke vragen
1.	Op welke wijze kan UWV WERKbedrijf de arbeidsmarkt via de haar beschikbare applicaties transparant maken waarbij de privacy van betrokkenen zo min mogelijk wordt geschonden?
2.	In welke mate voldoen SONAR en de dashboards aan de AVG zoals dat vertaald is in het Privacy Beleidskader?
3.	Voldoet SONAR aan de eisen van minimale gegevensverwerking (dataminimalisatie)?
4.	Worden niet meer gegevens verzameld, gebruikt of verstrekt dan noodzakelijk voor het doel?
5.	Staat de verwerking in redelijke verhouding tot het doel dat de verwerking dient?
6.	Indien bijzondere persoonsgegevens of het BSN worden verwerkt, kan het beoogde doel ook zonder deze gegevens worden bereikt?
7.	Hoe wordt binnen SONAR omgegaan met vrije invoervelden?
8.	[redacted] Art. 10 lid 2 sub e en g Wob
9.	Voldoet SONAR aan de eisen van Doelbinding en Proportionaliteit?
10.	Indien gegevens worden verwerkt voor een ander doel dan het oorspronkelijke doel, is dit doel dan verenigbaar met het oorspronkelijke doel?
16.	Worden de bewaar-/archiveringstermijnen (correct) gehandhaafd?
17.	Is voor alle gegevens in SONAR duidelijk wat de bewaartermijn is (volgens Selectielijst UWV WERKbedrijf)?
18.	Is in werkprocessen opgenomen wanneer een zaak is afgerond en de bewaartermijn ingaat?
19.	Is dit in metadatering opgenomen?
21.	Worden gegevens van een zaak die is afgerond overgebracht naar het archief?
23.	Worden de kopieën van gearchiveerde gegevens verwijderd?

#	UWV specifieke vragen
24.	Niet alleen uit SONAR en de dashboards, maar ook van andere opslaglocaties waar exportbestanden kunnen staan, zoals persoonlijke schijven, Outlook en SharePoint
25.	Hoe is geregeld dat gegevens na het verstrijken van de bewaartermijn worden vernietigd?
26.	Op welke wijze ondersteunen SONAR en de dashboards bij het voldoen aan verzoeken aan inzage- en correctierecht?
27.	Voldoen SONAR en de dashboards aan de vereisten op het gebied van beveiliging, naar de stand der techniek?
28.	Is duidelijk onder welke vertrouwelijkheidsklasse de persoonsgegevens vallen die worden verwerkt?
32.	Is in procesbeschrijvingen duidelijk vastgelegd onder welke omstandigheden hier gebruik van mag worden gemaakt, welke gegevens het mogen betreffen, waar deze gegevens worden opgeslagen, wie er toegang toe heeft, wat er met de gegevens mag worden gedaan en hoe wordt geborgd dat de gegevens tijdig verwijderd worden? En zijn deze afspraken voldoende bekend voor de uitvoerende medewerkers?
34.	Welke aanvullende (beveiligings)maatregelen dienen genomen te worden, indachtig de beginselen van privacy by design and default?
35.	Wat is op korte termijn te realiseren en welke elementen kunnen allicht beter meegenomen worden in de geplande vernieuwing van het applicatielandschap? (WorkIT)

Tabel 1: UWV WERKbedrijf privacyvragen

2.3 Object van onderzoek

De applicatie SONAR en de hierop betrekking hebbende processen en governance binnen UWV WERKbedrijf.

2.4 Scope en aanpak

Om te kunnen bepalen in welke mate SONAR voldoet aan de AVG hebben wij door middel van interviews en documentatiestudie een begrip gevormd van de informatiestromen, bedrijfsprocessen en de privacyprocessen van SONAR. Leidraad hierbij waren de door UWV WERKbedrijf opgestelde vragen en KPMG's Privacy Management Framework (zie Figuur 1). Het Privacy Management Framework is een geformaliseerd modulair raamwerk, bestaande uit de algemeen geaccepteerde privacyprincipes (GAPP) en andere elementen en subcomponenten, die de basis vormen voor privacyrisicobeheer binnen een organisatie. Wij hebben alle interviews gedocumenteerd en gevalideerd met de betreffende geïnterviewden. De geïnspecteerde documentatie vindt u in de Appendix Detailbevindingen. De Detailbevindingen zijn gevalideerd door de door UWV WERKbedrijf geïdentificeerde stakeholders (zie Tabel 1).

Figuur 2 KPMG's Privacy Management Framework

2.5 Beperkingen

Dit onderzoek is 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.

3 Belangrijkste bevindingen

3.1 UWV WERKbedrijf-specifieke vragen

Aan de hand van KPMG's Privacy Management Framework dat bestaat uit 12 domeinen hebben wij de privacyvolwassenheid van SONAR onderzocht. In de Detailbevindingen (zie Appendix) vindt u per domein de kracht, bevindingen, risico's en aanbevelingen. Naast een onderzoek naar de privacyvolwassenheid van SONAR, heeft het UWV WERKbedrijf een aantal specifieke vragen ter onderzoek voorgelegd. Een gedeelte van deze vragen komen aan bod in dit deelonderzoek. Wij hebben deze vragen gekoppeld aan KPMG's Privacy Management Framework en verwijzen voor de beantwoording derhalve naar het nummer van de detailbevinding in de Appendix.

#	Uw vraag	Observatie en referentie naar detailbevinding
1.	Op welke wijze kan UWV WERKbedrijf de arbeidsmarkt via de haar beschikbare applicaties transparant maken waarbij de privacy van betrokkenen zo min mogelijk wordt geschonden?	— Zie hiervoor de aanbevelingen in 5.1 t/m 5.4. — Het deelonderzoek IAM zal hier tevens nader op ingaan. — Duidelijk is dat de huidige wijze waarop de arbeidsmarkt transparant is gemaakt in SONAR de privacy van betrokkenen disproportioneel schaadt.
2.	In welke mate voldoen SONAR en de dashboards aan de AVG zoals dat vertaald is in het Privacy Beleidskader?	SONAR voldoet niet aan onderstaande AVG-vereisten: — Artikel 5 lid 1 sub a – rechtmatigheid (4.2) en transparantie (6.1). — Artikel 5 lid 1 sub b – doelbinding zie P5. — Artikel 5 lid 1 sub c – minimale gegevensverwerking (dataminimalisatie) P3. — Artikel 5 lid sub e – opslagbeperking (5.7). — Artikel 5 lid 1 sub f – passende technische en organisatorische maatregelen (8.1 t/m 8.4). — Artikel 32 – beveiliging van de verwerking (5.1 t/m 5.4 en 8.1 t/m 8.4).
3.	Voldoet SONAR aan de eisen van minimale gegevensverwerking (dataminimalisatie)?	— Nee. Zie hiervoor de bevindingen 5.1 t/m 5.4, 5.7 en 5.8. — Doordat medewerkers toegang hebben tot gegevens zonder dat zij dit nodig hebben voor de uitoefening van hun functie, wordt hier niet aan voldaan.
4.	Worden niet meer gegevens verzameld, gebruikt of verstrekt dan noodzakelijk voor het doel?	Zie hierboven bij nummer 3.
5.	Staat de verwerking in redelijke verhouding tot het doel dat de verwerking dient?	— Nee. UWV WERKbedrijf is hierover niet in controle, omdat er geen fijnmazig register gegevensverwerkingen is waarin dit beoordeeld

#	Uw vraag	Observatie en referentie naar detailbevinding	
		kan worden, en er geen GEB's zijn gedaan op bestaande SONAR-processen (2.1 en 7.1). — [redacted] en is er geen controle op doelbinding van vrije invoervelden (5.6). — Ook de te ruime toegangsrechten (5.1 t/m 5.4) betekenen dat de verwerking niet in verhouding staat tot het doel.	Art. 10 lid 2 sub e en g Wob
6.	Indien bijzondere persoonsgegevens of het BSN worden verwerkt, kan het beoogde doel ook zonder deze gegevens worden bereikt?	— Ja. Zie 4.2 en 10.1. — In workarounds komt het voor dat exports weer worden verrijkt met BSN-nummers, zonder duidelijke noodzaak.	
7.	Hoe wordt binnen SONAR omgegaan met vrije invoervelden?	[redacted]	Art. 10 lid 2 sub e en g Wob
8.	[redacted]	[redacted]	Art. 10 lid 2 sub e en g Wob
9.	Voldoet SONAR aan de eisen van Doelbinding en Proportionaliteit?	Nee, zie P2 en P5.	
10.	Indien gegevens worden verwerkt voor een ander doel dan het oorspronkelijke doel, is dit doel dan verenigbaar met het oorspronkelijke doel?	— Nee, zie 5.8 en 8.3. — Omdat veel buiten SONAR om wordt gewerkt met SONAR-data is er geen grip op de secundaire doelen. — [redacted] — [redacted]	Art. 10 lid 2 sub e en g Wob
16.	Worden de bewaar-/archiveringstermijnen (correct) gehandhaafd?	Nee. Zie 5.7.	
17.	Is voor alle gegevens in SONAR duidelijk wat de bewaartermijn is (volgens Selectielijst UWV WERKbedrijf)?	Nee, zie 5.7.	
18.	Is in werkprocessen opgenomen wanneer een zaak is afgerond en de bewaartermijn ingaat?	Nee. Zie 5.7.	

#	Uw vraag	Observatie en referentie naar detailbevinding
19.	Is dit in metadatering opgenomen?	Dit is niet in de metadatering opgenomen. Voor informatie over klanten en klantaccounts in het geheel geldt dat deze niet automatisch verwijderd worden. In plaats daarvan moet een script gedraaid worden. De laatste keer dat dit script gedraaid werd, waren er veel foutmeldingen, waardoor een aantal verwijderde data teruggezet moest worden. Het verwijderen van data in SONAR kost aldus veel capaciteit, waar geen prioriteit aan gegeven wordt.
21.	Worden gegevens van een zaak die is afgerond overgebracht naar het archief?	Nee. Zie 5.7.
23.	Worden de kopieën van gearchiveerde gegevens verwijderd?	Tot op heden nog niet. Er is een project gaande waarin documenten centraal gearchiveerd zullen worden. Dit geldt alleen voor de documenten en bijlagen die in SONAR opgeslagen zijn. Voor alle andere klantgegevens is nog geen verwijderplan opgesteld, anders dan de verwijderscripts die gedraaid zouden moeten worden, maar vaak door lage prioritering uitgesteld worden.
24.	Niet alleen uit SONAR en de dashboards, maar ook van andere opslaglocaties waar exportbestanden kunnen staan, zoals persoonlijke schijven, Outlook en SharePoint	— Exports vanuit SONAR worden op de harde schijf opgeslagen en niet (altijd) verwijderd. — Zie 10.1.
25.	Hoe is geregeld dat gegevens na het verstrijken van de bewaartermijn worden vernietigd?	Gegevens in SONAR zijn in het verleden ‘ad hoc’ verwijderd. De laatste keer dat dit gebeurde, ging er veel mis, waardoor veel scripts teruggedraaid moesten worden. Het staat laag op de agenda om op te lossen.
26.	Op welke wijze ondersteunen SONAR en de dashboards bij het voldoen aan verzoeken aan inzage- en correctierecht?	Zie 7.2.
27.	Voldoen SONAR en de dashboards aan de vereisten op het gebied van beveiliging, naar de stand der techniek?	Nee, zie 5.5 en 8.1 t/m 8.4.
28.	Is duidelijk onder welke vertrouwelijkheidsklasse de persoonsgegevens vallen die worden verwerkt?	Niet op een fijnmazig genoeg niveau, zie 2.2.
32.	Is in procesbeschrijvingen duidelijk vastgelegd onder welke omstandigheden hier gebruik van mag worden gemaakt, welke gegevens het mogen betreffen, waar deze gegevens worden opgeslagen, wie er toegang toe heeft, wat er met de gegevens mag worden gedaan en hoe wordt geborgd dat de gegevens tijdig verwijderd worden? En zijn deze afspraken voldoende bekend voor de uitvoerende medewerkers?	Nee, zie 2.1, 2.2, 5.7 en 10.1.

#	Uw vraag	Observatie en referentie naar detailbevinding
34.	Welke aanvullende (beveiligings)maatregelen dienen genomen te worden, indachtig de beginselen van privacy by design and default?	Zie de aanbevelingen van de detailbevindingen, o.a. 5.1 t/m 5.9 en 8.1 t/m 8.4.
35.	Wat is op korte termijn te realiseren en welke elementen kunnen allicht beter meegenomen worden in de geplande vernieuwing van het applicatielandschap? (WorkIT)	— Hiervoor verwijzen we naar de Management-samenvatting. Op korte termijn is waarschijnlijk slechts een beperkte set aan maatregelen te realiseren, waardoor de risico's niet effectief gemitigeerd kunnen worden. — WorkIT kan verbeteringen brengen met betrekking tot het veilig versturen van berichten, en het archiveren van documenten (maar niet van klanten) in SONAR. Ook kan de toegang tot SONAR voor sommige medewerkers ontzegd worden als eAfspraak met WorkIT geïmplementeerd is. — De ondubbelzinnige toezegging voor structurele verbetering.

Tabel 1 UWV WERKbedrijf's privacyvragen en KPMG's observaties

3.2 KPMG's Privacy Management Raamwerk

Hoewel binnen UWV en binnen UWV WERKbedrijf over het algemeen processen formeel gedocumenteerd zijn, ontbreekt het aan documentatie en formele controlemaatregelen om een effectieve operatie van processen te waarborgen. Het volwassenheidsniveau van SONAR is voor de meeste domeinen 'herhaalbaar', voor vier domeinen 'initieel', en voor twee 'gedefinieerd'. Gezien de gevoeligheid, hoeveelheid persoonsgegevens, en het grote aantal gebruikers in SONAR, verwachten wij voor alle domeinen ten minste een volwassenheidsniveau van 'gedefinieerd'. Voor de details per domein, verwijzen wij naar de appendix.

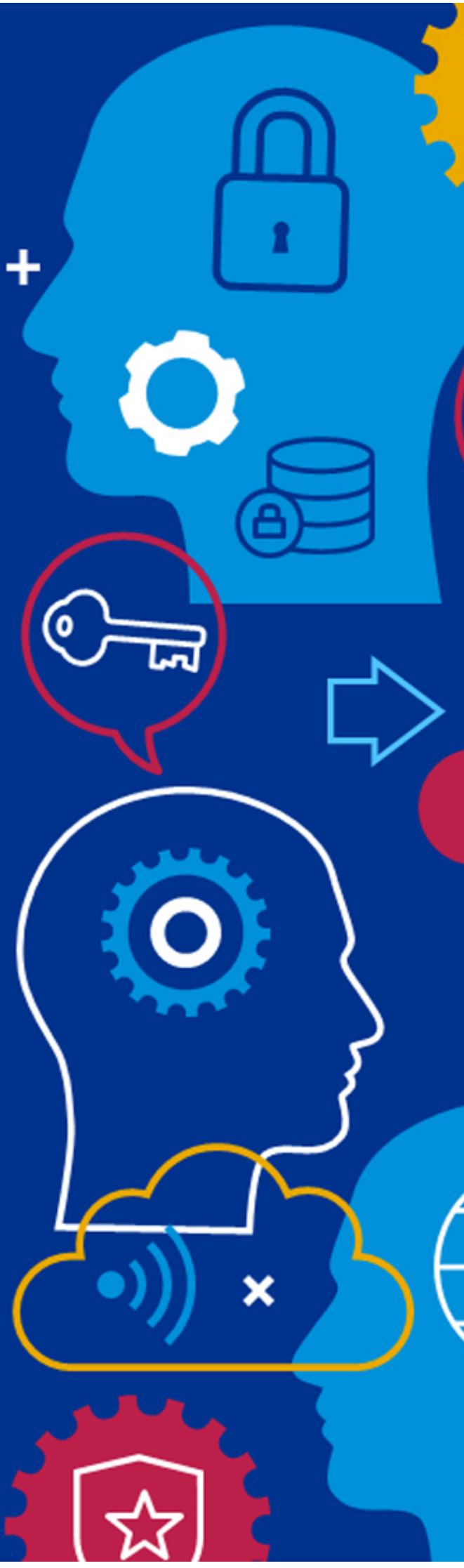
Domein	Inschatting volwassenheidsniveau					Bevindingen			
						H	M	L	Σ
Governance and Operating model	Initieel	**Herhaalbaar**	Gedefinieerd	Gemanaged	Geoptimali-seerd	2			**2**
Inventory & Data Mapping	Initieel	**Herhaalbaar**	Gedefinieerd	Gemanaged	Geoptimali-seerd	1	1		**2**
Risk and Control	Initieel	**Herhaalbaar**	Gedefinieerd	Gemanaged	Geoptimali-seerd	3			**3**
Regulatory Management	Initieel	**Herhaalbaar**	Gedefinieerd	Gemanaged	Geoptimali-seerd	2	1		**3**
Information Life Cycle Management	**Initieel**	Herhaalbaar	Gedefinieerd	Gemanaged	Geoptimali-seerd	9			**9**
Policies	Initieel	Herhaalbaar	**Gedefinieerd**	Gemanaged	Geoptimali-seerd	1			**1**
Processes, Procedures and Technology	Initieel	Herhaalbaar	**Gedefinieerd**	Gemanaged	Geoptimali-seerd		1	1	**2**
Security for Privacy	Initieel	**Herhaalbaar**	Gedefinieerd	Gemanaged	Geoptimali-seerd	3	1		**4**
Third Party Management	Initieel	**Herhaalbaar**	Gedefinieerd	Gemanaged	Geoptimali-seerd		1		**1**
Training and Awareness	Initieel	**Herhaalbaar**	Gedefinieerd	Gemanaged	Geoptimali-seerd	1	1		**2**
Monitoring	**Initieel**	Herhaalbaar	Gedefinieerd	Gemanaged	Geoptimali-seerd	1	1		**2**
Incident Management	**Initieel**	Herhaalbaar	Gedefinieerd	Gemanaged	Geoptimali-seerd	2			**2**
					Totaal:	**25**	**7**	**1**	**33**

Tabel 2 Privacyvolwassenheidsniveau van SONAR per domein

Appendices

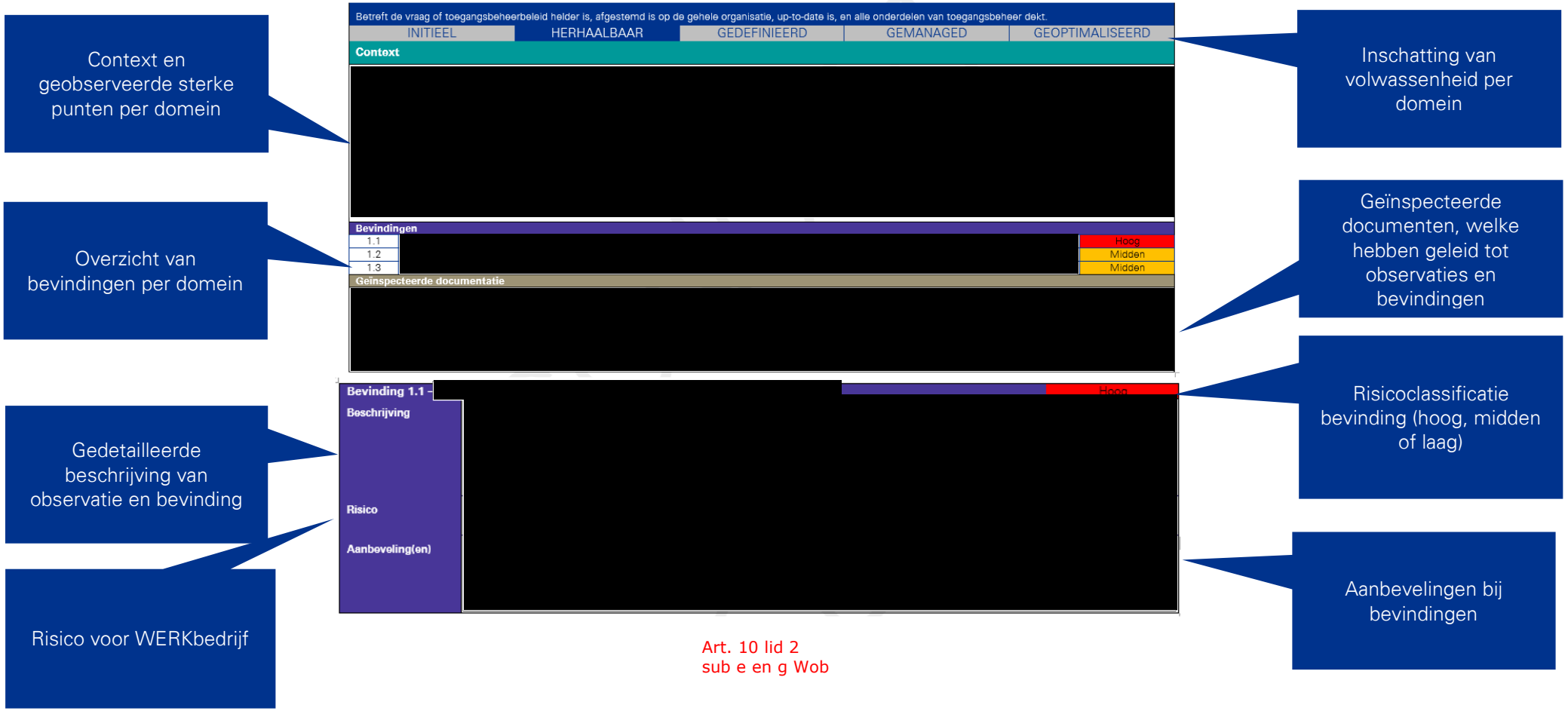
A Gedetailleerde resultaten volwassenheidsmeting

B Lijst van geïnterviewden



A: Gedetailleerde resultaten volwassenheidsmeting

In dit hoofdstuk wordt per domein in detail beschreven waar het domein precies over gaat, wat de sterke punten van het UWV WERKbedrijf zijn op dit domein en welke bevindingen er bij een domein horen. In de afbeelding hieronder wordt toegelicht hoe de detailbevindingen zijn opgebouwd.



Art. 10 lid 2
sub e en g Wob

1. Governance and Operating Model

De benodigde organisatiestructuur en de vastgelegde en vervulde rollen en verantwoordelijkheden bij het verzamelen, gebruiken, bewaren, delen en verwijderen van persoonsgegevens.				
INITIEEL	HERHAALBAAR	GEDEFINIEERD	GEMANAGED	GEOPTIMALISEERD

Context

De UWV-brede privacyorganisatiestructuur bestaat uit de Functionaris Gegevensbescherming (FG) die als derde lijn toezicht houdt en het Bureau Gegevensbescherming (BG) dat als tweede lijn het beleid uitzet. De verantwoordelijkheid, risicoafweging en implementatie met betrekking tot privacy is een lijnverantwoordelijkheid van de divisie en ligt voor SONAR bij (de directie van) UWV WERKbedrijf. Het team Informatiebeveiliging en Privacy (hierna: IB&P) functioneert binnen UWV WERKbedrijf als tweede lijn. Er zijn echter in de eerste lijn van UWV WERKbedrijf (zowel binnen de regiokantoren als binnen de applicatie SONAR) onvoldoende privacyrollen en -verantwoordelijkheden belegd om privacyrisico's effectief te kunnen beheersen. Daarnaast wordt geen of onvoldoende geen eigenaarschap van privacyrisico's genomen.

Bevindingen

1.1	Er zijn onvoldoende privacyrollen en -verantwoordelijkheden in de eerste lijn belegd om privacyrisico's effectief te kunnen beheersen	Hoog
1.2	Er wordt geen of onvoldoende eigenaarschap van privacyrisico's in SONAR genomen	Hoog

Bevinding 1.1 – Onvoldoende privacyrollen en -verantwoordelijkheden in de eerste lijn belegd om privacyrisico's effectief te kunnen beheersen	Hoog
Beschrijving	**Regiokantoren** Werknemers van regiokantoren begrijpen soms onvoldoende waarom privacy belangrijk is (zie ook onder 10). Wij zijn geïnformeerd dat er veel weerstand is als er privacymaatregelen worden genomen. Daardoor komen er vaak workarounds voor. Eén van de hoofdoorzaken is het gebrek aan een privacycontactpunt binnen de regiokantoren, waardoor er weinig grip is op de omgang met persoonsgegevens aldaar. **Applicatie governance** In de applicatie zijn geen privacy-KPI's of -rollen belegd, bijvoorbeeld bij de product owner. Gezien de inherent hoge privacyrisico's van SONAR, zoals de verwerking van gevoelige gegevens van een kwetsbare groep betrokkenen, waar veel UWV WERKbedrijf-medewerkers en ketenpartners toegang toe hebben, is een sterke verankering van privacy in de applicatie governance noodzakelijk. Deze ontbreekt momenteel.
Risico	Het risico is dat activiteiten die ondernomen moeten worden om de privacyrisico's te mitigeren, niet genomen worden, of niet effectief zijn.
Aanbeveling(en)	Wij adviseren: 1 Zorg ervoor dat er in de regiokantoren een sterker verankerd privacynetwerk is, bijvoorbeeld door 'privacy champions' te benoemen. 2 Zorg daarnaast voor formele privacycompetentieprofielen of -KPI's, voor zowel de operationeel manager als voor rollen binnen het applicatiebeheer van SONAR.

Bevinding 1.2 – Er wordt geen of onvoldoende eigenaarschap van privacyrisico's in SONAR genomen	Hoog	
Beschrijving	Risico-eigenaar van SONAR is de [redacted], en het DT UWV WERKbedrijf. Voor veel risico's die bekend zijn in SONAR (zie ook onder 8), zijn geen of beperkte maatregelen genomen. Wij hebben geen documentatie ontvangen waarin deze privacyrisico's bewust zijn afgewogen en geaccepteerd door de risico-eigenaren.	Art. 10 lid 2 sub e Wob
Risico	[redacted]	Art. 11 lid 1 Wob
Aanbeveling(en)	Wij adviseren: 1 Creëer een risicomanagementproces, in samenhang met het nieuwe bestuurslid dat risk and compliance in de portefeuille zal krijgen	

2. Data Inventory and Mapping

Een register van de verwerkingsactiviteiten van persoonsgegevens, waaronder: welke persoonsgegevens worden verzameld, met welk doel, waar deze worden opgeslagen en aan wie deze worden overgedragen/gedeeld (artikel 30 AVG).				
INITIEEL	HERHAALBAAR	GEDEFINIEERD	GEMANAGED	GEOPTIMALISEERD

Context

UWV WERKbedrijf heeft een register van verwerkingsactiviteiten dat van heel UWV WERKbedrijf de processen beschrijft. Dit is door het BG opgesteld dat ook het eigenaarschap over het document heeft. De verwerkingen bevatten een grondslag, categorie betrokkenen, categorieën persoonsgegevens, ontvangers en internationale doorgiften. Daarnaast bevat het register een algemene beschrijving van bewaartermijnen en technische en organisatorische maatregelen.

Bevindingen		
2.1	Het register is te grofmazig om te kunnen bepalen of persoonsgegevens onrechtmatig worden verwerkt	Hoog
2.2	Dataclassificatie is niet vastgesteld op adequaat niveau	Midden

Bevinding 2.1 – Het register is te grofmazig om te kunnen bepalen of persoonsgegevens onrechtmatig worden verwerkt	Hoog
Beschrijving	Het register is te grofmazig en niet up-to-date. Er wordt niet omschreven welke verwerkingen binnen SONAR plaatsvinden, noch welke persoonsgegevens in SONAR worden verwerkt. Er is geen proces om ervoor te zorgen dat de lijn het register up-to-date houdt. Daarnaast is het register onvolledig en soms onjuist. Zo ontbreken bijvoorbeeld categorieën kwetsbare groepen, zoals kinderen, niet-uitkeringsgerechtigden en bijstandsgerechtigden.
Risico	Het risico is dat het niet mogelijk is om te bepalen of persoonsgegevens onrechtmatig worden verwerkt, of er voor iedere verwerking doelbinding is, en of iedere verwerking in overeenstemming is met het beginsel van minimale gegevensverwerking.
Aanbeveling(en)	Wij adviseren: 1 Classificeer data binnen SONAR en neem passende maatregelen om ervoor te zorgen dat passende bescherming geboden wordt om de persoonsgegevens naar classificatie te beschermen.

Bevinding 2.2 – Dataclassificatie is niet vastgesteld op adequaat niveau	Midden
Beschrijving	Er is een dataclassificatielijst opgesteld voor UWV WERKbedrijf, maar deze is te grofmazig om te kunnen koppelen aan de persoonsgegevens die op applicatieniveau verwerkt worden. Daarnaast is de dataclassificatie niet gekoppeld aan (minimaal) te nemen maatregelen. Aan "Gegevens over arbeidsrelatie(s) of klantrelatie" is, gezien de gevoeligheid, een te lage classificering (1 van 0 t/m 3) toegekend. Hieronder vallen zeer gevoelige gegevens, zoals de sociale context van een klant. Dataclassificatie is vastgesteld binnen SONAR, maar er zijn geen maatregelen genomen om op basis van dataclassificatie de meer gevoelige persoonsgegevens beter te beschermen.
Risico	Het risico is dat persoonsgegevens onzorgvuldig worden verwerkt of dat ze niet de juiste mate van bescherming krijgen, omdat de persoons-gegevens niet of onjuist zijn geclassificeerd.
Aanbeveling(en)	Wij adviseren: 1 Wijs een eindverantwoordelijke aan voor toegangsbeheer SONAR. 2 Neem de bijbehorende taken op in functieomschrijving van die eindverantwoordelijke. 3 Stel een richtinggevende lange-termijn strategie op voor toegangsbeheer binnen SONAR en werk die toe naar concreet beleid en acties voor functioneel beheer en andere stakeholders.

3. Risk & Control

De manier waarop privacyrisico's voor de organisatie worden vastgelegd en bijgehouden, en de acties die ondernomen worden om de risico's te mitigeren of in controle te blijven over risico's, waarbij bewuste afwegingen over (rest)risico's worden gemaakt.				
INITIEEL	HERHAALBAAR	GEDEFINIEERD	GEMANAGED	GEOPTIMALISEERD

Context

Risicomanagement is nog niet ingericht in UWV WERKbedrijf. Wel is dit een doelstelling uit het (nog niet gefinaliseerde) IBP jaarplan 2020 van UWV WERKbedrijf, maar op dit moment is er geen inventarisatie gemaakt van de privacyrisico's voor UWV WERKbedrijf. Het BG heeft een UWV-breed Beleidskader Privacy opgesteld, waaraan de onderliggende divisies zich moeten toetsen. UWV WERKbedrijf heeft dit echter tot op heden niet gedaan. Het BG heeft zogenaamde GEB's ontworpen als beoordelingsmethodologie van privacyrisico's voor nieuwe verwerkingen. Voor SONAR is er echter nooit een GEB uitgevoerd. Wel zijn een aantal SONAR-risico's op andere manieren aan het licht gebracht, zoals door de onderzoeken van de toezichthouder, het hoge aantal datalekken, en interne onderzoeken. De risico's worden niet tijdig en effectief gemitigeerd.

Bevindingen		
3.1	UWV WERKbedrijf (WB) is niet in controle over privacyrisico's in SONAR	Hoog
3.2	Divisie UWV WERKbedrijf heeft privacyrisico's niet beoordeeld aan het Beleidskader Privacy of de AVG	Hoog
3.3	Reeds gerapporteerde privacyrisico's van SONAR worden niet tijdig en effectief gemitigeerd	Hoog

Bevinding 3.1 – UWV WERKbedrijf (WB) is niet in controle over privacyrisico's in SONAR	Hoog
Beschrijving	Ondanks bekende privacyrisico's van SONAR, is UWV WERKbedrijf hierover niet in controle. UWV WERKbedrijf (DT) heeft geen expliciete privacyvisie opgesteld, in lijn met de UWV-brede visie. De BSO van UWV WERKbedrijf heeft een jaarplan opgesteld, maar dat van 2019 is nooit gefinaliseerd of goedgekeurd door het DT. Voor het jaarplan van 2020 staat goedkeuring gepland in Q1. Specifiek voor SONAR is een visiedocument opgesteld waarin uitfasering als beste van drie scenario's wordt aanbevolen. Dit is echter niet gefinaliseerd noch goedgekeurd door het DT. Het regieprogramma WorkIT bevat weinig concrete en tijdgebonden stappen voor 2019 en 2020 ten behoeve van specifieke privacyrisico's in SONAR.
Risico	Het risico is dat zonder een gedefinieerde privacy-ambitie SONAR blootgesteld wordt aan een hoger privacyrisico dan door de organisatie gewenst is. Daarnaast is het risico is dat zonder duidelijke visie en strategie van het DT, de BSO niet de draagkracht en het mandaat heeft om benodigde veranderingen in de organisatie te kunnen doorvoeren.
Aanbeveling(en)	Wij adviseren: 1 Maak privacy een vast onderdeel van de DT-agenda. 2 Stel daarnaast een korte en lange termijn privacyvisie en -ambitie op voor het WB, in lijn met het UWV-brede beleid. Koppel hieraan een privacystrategie, inclusief de benodigde budgets, resourcing en KPI's.

Bevinding 3.2 – UWV WERKbedrijf heeft geen gap-analyse ten opzichte van het privacybeleidskader uitgevoerd	Hoog
Beschrijving	Iedere divisie is verantwoordelijk voor het uitvoeren van een gap-analyse ten opzichte van het Privacy Beleidskader. UWV WERKbedrijf heeft deze echter tot op heden niet uitgevoerd. Voorliggend onderzoek wordt als eerste stap hiervan gezien, maar dit ziet slechts op één applicatie van UWV WERKbedrijf.
Risico	Het risico is dat er onvoldoende maatregelen ten behoeve van privacy worden getroffen om persoonsgegevens adequaat te beschermen.
Aanbeveling(en)	Wij adviseren: 1 Identificeer, documenteer (bijvoorbeeld in een risicoregister) en beoordeel de privacyrisico's waaraan UWV WERKbedrijf is blootgesteld, inclusief de adequate maatregelen om de geïdentificeerde risico's te beheersen. Start een periodieke (interne en/of externe) privacy audit-cyclus voor UWV WERKbedrijf.

Bevinding 3.3 – Reeds gerapporteerde privacyrisico's in SONAR worden niet, niet tijdig of niet effectief gemitigeerd	Hoog
Beschrijving	Door verschillende interne stakeholders en de toezichthouder zijn risico's van SONAR geïdentificeerd. Dit heeft echter beperkt geleid tot het nemen van effectieve mitigerende maatregelen. De risicobereidheid van de directie WB lijkt daardoor hoog, in tegenstelling tot de visie in het Strategisch Beleid Informatiebeveiliging en Privacy (IB&P) waarin staat: "Het is onze plicht die informatie goed te beveiligen en de privacy van onze klanten te respecteren."
Risico	[redacted] Art. 11 lid 1 Wob
Aanbeveling(en)	Wij adviseren: 1 Zorg ervoor dat privacyrisico's in SONAR het juiste gewicht krijgen, bijvoorbeeld door middel van een risicoregister als beschreven in 3.1. Het is van belang dat de geïdentificeerde risico's een plan-do-check-actcyclus kennen, om te waarborgen dat de maatregelen effectief zijn en blijven.

4. Regulatory Management

De wettelijke grondslag waarop de verwerking van persoonsgegevens is gebaseerd, en het proces bij internationale doorgiften (indien van toepassing).					
INITIEEL	HERHAALBAAR	GEDEFINIEERD	GEMANAGED	GEOPTIMALISEERD	
Context					
Het register verwerkingsactiviteiten bevat UWV-breed per hoofdproces de wettelijke grondslag (i.h.k.v. UWV WERKbedrijf met name SUWI, Wajong, Wmo, WIA, Participatiewet). Specifiek voor SONAR zijn de grondslagen van de verwerkingen echter niet gedocumenteerd (zie onder 2). Sommige verwerkingen in SONAR hebben geen wettelijke grondslag. Daarnaast wordt de Wet SUWI onterecht als excuus gebruikt voor de te ruime inrichting van toegangs- en inzagerechten.					
Bevindingen					
4.1	De transparante arbeidsmarkt van de Wet SUWI is geen grondslag op basis waarvan toegang en inzage niet of nauwelijks beperkt hoeven te worden in SONAR (zie ook onder 5)			Hoog	Art. 10 lid 2 sub e en g Wob
[redacted]					
4.3	Toestemming wordt onnodig als grondslag gebruikt voor sommige verwerkingen in SONAR			Midden	

Bevinding 4.1 – De transparante arbeidsmarkt van de Wet SUWI is geen grondslag op basis waarvan toegang en inzage niet of nauwelijks beperkt hoeven te worden in SONAR (zie ook onder 5)	Hoog
Beschrijving	Een reden die door UWV WERKbedrijf vaak wordt genoemd om de toegangs- en inzagerechten in SONAR niet te (kunnen) beperken is de uitvoering van UWV's wettelijke taak om de landelijke arbeidsmarkt transparant te maken. Dat betekent dat bepaalde medewerkers op grond van deze wettelijke taak landelijk inzage in SONAR nodig hebben. Ten onrechte wordt op dit moment aangenomen dat landelijk betekent dat alles open moet zijn en dat privacy betekent dat alles dicht moet zijn. Het is echter niet zo binair.
Risico	Het risico van de wettelijke taak ruim opvatten is dat er geen of nauwelijks maatregelen worden genomen om de inbreuk op de persoonlijke levenssfeer van de betrokkenen te beperken.
Aanbeveling(en)	Wij adviseren: 1 Zorg ervoor dat de opvatting van de wettelijke taak in lijn is met noodzakelijkheid en doelbinding, resulterend in passende maatregelen in SONAR: de toegang dient beperkt te worden in lijn met de beginselen van proportionaliteit en noodzakelijkheid. Dit vergt een herbeoordeling van de toegangsrechten tot en binnen SONAR voor de gebruikers van UWV WERKbedrijf, overige UWV-divisies en gemeentes. Zo kan de bijvoorbeeld de landelijk inzage in SONAR beperkt te worden tot alleen die medewerkers die dat nodig hebben voor de uitvoering van hun werkzaamheden.

[redacted]

Art. 10 lid 2 sub e en g Wob

Bevinding 4.3 – Toestemming wordt onnodig als grondslag gebruikt voor sommige verwerkingen in SONAR	Midden
Beschrijving	Toestemming wordt onnodig gevraagd voor het delen van cv's met externe partijen (werkgevers met concrete vacatures, maar ook commerciële uitzendbureaus) en voor het extern inkopen van een re-integratietraject, waarbij het gemaakte werkplan ook naar het re-integratiebureau wordt gezonden. Preambule 43 van de AVG en de AP expliciteren dat toestemming van een overheidsorgaan, zeker omdat er een ondergeschiktheids-relatie is tussen klant en UWV WERKbedrijf doordat de klant afhankelijk is van de uitkering, niet vrijelijk gegeven kan worden, en daarmee niet geldig is. In het geval van de commerciële uitzendbureaus is daarnaast de toestemming ook niet voldoende specifiek. Tot slot wordt de toestemming niet vastgelegd, waardoor niet aangetoond kan worden dat toestemming verleend is. UWV WERKbedrijf deelt cv's op basis van een andere wettelijke grondslag dan toestemming en daarom is het vragen van toestemming onnodig.
Risico	[redacted] Art. 11 lid 1 Wob
Aanbeveling(en)	Wij adviseren: 1 Onderzoek alle verwerkingen waarvoor toestemming wordt gevraagd en beoordeel of deze vrijelijk, specifiek, en ondubbelzinnig gegeven wordt. 2 Houd daarbij in het bijzonder rekening met toestemming die voor meer dan één werkgever of uitzendbureau is. Informeer de betrokkenen daarnaast goed als toestemming gevraagd wordt, en zorg ervoor dat toestemming vastgelegd wordt.

5. Data Lifecycle Management

De processen en controles rondom persoonlijke informatie tijdens de hele levenscyclus (van verzameling tot gebruik, bewaring, openbaarmaking en vernietiging).				
INITIEEL	HERHAALBAAR	GEDEFINIEERD	GEMANAGED	GEOPTIMALISEERD

Context

In SONAR is een aantal maatregelen getroffen die de openbaarmaking en bewaring van persoonsgegevens beperken: Zo wordt binnen SONAR onderscheid gemaakt in lees- en schrijfrechten. Ook wordt data van overleden personen gemaskeerd. Vanuit SONAR wordt communicatie (zoals brieven) zonder BSN verstuurd. Daarnaast bevat een export uit SONAR via de BI-dashboards geen BSN en NAW meer. Ook is het niet meer mogelijk om een databasebestand te uploaden in de werkmap. Op dit moment loopt een proef voor het regionaal autoriseren voor gemeentes.

Bevindingen		
5.1	Nagenoeg alle gebruikers van SONAR hebben dezelfde leesrechten: Landelijk/regionaal	Hoog
5.2	Nagenoeg alle gebruikers van SONAR hebben dezelfde leesrechten: Gemeentes, derde partijen en overige gebruikers	Hoog
5.3	Nagenoeg alle gebruikers van SONAR hebben dezelfde leesrechten: Aantal gegevensvelden en gebruik ervan	Hoog
5.4	Nagenoeg alle gebruikers van SONAR hebben dezelfde leesrechten: Tabbladen	Hoog
5.5	Maatregel BI-dashboards naar aanleiding van datalek dekt maar een gedeelte van het risico af	Hoog
5.6	Er zijn geen effectieve maatregelen om de risico's van vrije invoervelden te beperken	Hoog
5.7	SONAR-gegevens worden niet of nauwelijks meer geschoond	Hoog
5.8	Lokale opslag van SONAR-data	Hoog
[redacted]		

Art. 10 lid 2
sub e en g Wob

Bevinding 5.1 – Nagenoeg alle gebruikers van SONAR hebben dezelfde leesrechten: Landelijk/regionaal	Hoog	
Beschrijving	Nagenoeg alle gebruikers van SONAR hebben dezelfde leesrechten. In het kader van de uitvoering van de wettelijke taak, namelijk het transparant maken van de arbeidsmarkt en het bemiddelen van werkzoekenden naar de arbeidsmarkt, heeft een deel van de gebruikers landelijk inzage in SONAR nodig. Dit geldt echter niet voor alle gebruikers: de toegang is niet beperkt op basis van het 'need-to-have' principe. In het geval dat inzage in persoonsgegevens van klanten buiten de regio niet noodzakelijk is, ontbreekt doelbinding en het beginsel van minimale gegevensverwerking (artikel 5 AVG).		
Risico	[redacted]		Art. 11 lid 1 Wob
Aanbeveling(en)	Wij adviseren het volgende: 1 Wij zijn geïnformeerd dat het inzien van klantgegevens buiten de regio voor de meeste functies niet per definitie een noodzakelijk is, maar in bepaalde gevallen wel. Rol daarom de proef "regionaal autoriseren" breed uit en beperk inzage in SONAR tot klantgegevens voor de gebruikers van SONAR die alleen regionaal inzage behoeven. De leidende gedachte hierbij zou moeten zijn 'Niet open, mits, maar dicht, tenzij'. Daarvoor kan verder de voorgestelde analyse in het Identity en Access Management deelonderzoek worden ingezet.		

Bevinding 5.2 – Nagenoeg alle gebruikers van SONAR hebben dezelfde leesrechten: Gemeentes, derde partijen en overige gebruikers	Hoog	
Beschrijving	SONAR heeft ongeveer 15.000 gebruikers, waarvan de helft gebruikers van UWV WERKbedrijf en gemeentes. De overige gebruikers zijn o.a. medewerkers van andere divisies binnen het UWV. Van de 15.000 gebruikers heeft een deel landelijk inzage in SONAR nodig om de wettelijke taak te kunnen uitvoeren, maar dat geldt niet voor alle gebruikers. Gemeentes hebben in beginsel alleen toegang nodig tot SONAR ten behoeve van klanten voor hun eigen gemeente. Hier geldt dat inzage in klanten van andere gemeentes niet noodzakelijk en niet proportioneel is. Hetzelfde geldt voor overige partijen en gebruikers van andere divisies binnen het UWV met toegang tot SONAR. Voor deze groep gebruikers geldt geen of minimale beperking tot de inzage van alle klantgegevens in SONAR. Het openzetten van de toegang tot een te grote groep gebruikers voldoet niet aan het beginsel van minimale gegevensverwerking (artikel 5 AVG) en daarmee ook niet aan de AVG.		
Risico	[redacted]		Art. 11 lid 1 Wob

Aanbeveling(en)	Wij adviseren: 1 Zorg ervoor dat de inzage in SONAR beperkt is tot wat noodzakelijk is voor de uitvoering van de werkzaamheden van de medewerkers. [redacted]

Art. 10 lid 2 sub e en g Wob

Bevinding 5.3 – Nagenoeg alle gebruikers van SONAR hebben dezelfde leesrechten: Gegevensvelden en gebruik ervan	Hoog
Beschrijving	SONAR telt rond de 630 gegevens met daarin persoonsgegevens (en overige gegevens) van werkzoekenden, maar ook van bijstandsgerechtigden, kinderen en kwetsbare groepen in het kader van de Wajong, WIA en Participatiewet. In SONAR is autorisatie ingedeeld in rollen. De voornaamste rollen zijn adviseur basis, adviseur intensief en adviseur WSP. Ondanks verschillende rollen is de inzage in de gegevens niet technisch gescheiden. Een adviseur basis kan ook gegevens inzien van een adviseur intensief die in feite niets met de functie van adviseur basis te maken heeft. De verwerking voldoet daarmee niet aan het beginsel van minimale gegevensverwerking (artikel 5 AVG).
Risico	[redacted]
Aanbeveling(en)	Wij adviseren: 1 Beperk de inzage in klantgegevens voor de verschillende rollen binnen UWV WERKbedrijf en de gemeentes, afhankelijk van functie, type klant, type dienstverlening en regio.

Art. 10 lid 2 sub e en g Wob

Bevinding 5.4 – Nagenoeg alle gebruikers van SONAR hebben dezelfde leesrechten: Tabbladen	Hoog
Beschrijving	De leesrechten binnen SONAR zijn niet of nauwelijks beperkt. Sommige tabbladen in SONAR bevatten meer gevoelige gegevens van persoonlijke aard dan andere tabbladen. De inzage in verschillende tabbladen is niet of nauwelijks beperkt. Niet voor alle gebruikers van SONAR is toegang tot alle tabbladen noodzakelijk. Een voorbeeld is het tabblad Voorzieningen dat alleen gebruikt wordt door de medewerkers die binnen dit proces werken.
Risico	[redacted]
Aanbeveling(en)	Wij adviseren: 1 Beperk de toegang tot verschillende tabbladen, afhankelijk van het type klant, type dienstverlening en regio, met name voor tabbladen die gevoelig zijn zoals het tabblad Voorzieningen. Dataclassificatie kan hierbij hulp bieden.

Art. 10 lid 2 sub e en g Wob

Bevinding 5.5 – Maatregel BI-dashboards naar aanleiding van datalek dekt maar een gedeelte van het risico af	Hoog
Beschrijving	Naar aanleiding van een aantal datalekken heeft UWV WERKbedrijf de maatregel getroffen om het aantal persoonsgegevens in het BI-dashboard te minimaliseren. Zo zijn BSN en NAW-gegevens niet meer zichtbaar. Deze maatregel heeft een beperkte werking, want de leesrechten in de applicatie zelf worden daarmee niet beperkt. BSN zijn nog steeds op te zoeken. Ook vanuit SONAR zelf kan men data exporteren.
Risico	Het risico bestaat dat personeel buiten SONAR om verschillende gegevens combineert tot weer een volledige set en deze gegevens buiten de beheersingsmaatregelen van de applicatie houdt.
Aanbeveling(en)	Wij adviseren: 1 Dit risico blijft bestaan zolang SONAR gebruikt wordt. Uit documentatie blijkt dat een groot deel van de dienstverlening komt stil te liggen wanneer de exports uit SONAR onmogelijk gemaakt worden.

Bevinding 5.6 – Er zijn geen effectieve maatregelen om de risico's van vrije invoervelden te beperken	Hoog	
Beschrijving	[redacted] Niet alle medewerkers zijn op de hoogte van de instructie op welke wijze informatie genoteerd mag worden. Er worden geen controles uitgevoerd op de wijze waarop in de toelichtingen informatie over de klant beschreven wordt.	Art. 10 lid 2 sub e en g Wob
Risico	[redacted]	Art. 10 lid 2 sub e en g Wob
Aanbeveling(en)	Wij adviseren: 1 Geef duidelijke instructies over het invullen van vrije invoervelden en laat de lijn periodiek monitoren, bijvoorbeeld door de 'privacy champion'.	

Bevinding 5.7 – SONAR-gegevens worden niet of nauwelijks meer geschoond	Hoog
Beschrijving	SONAR is sinds implementatie beperkt geschoond en een deel van de data sinds 2018 helemaal niet meer door technische beperkingen. Daarnaast wordt SONAR als archiveringssysteem gebruikt. Als gevolg daarvan bevat SONAR een zeer groot aantal persoonsgegevens van zowel actieve als inactieve klanten, die ingezien kunnen worden door de gebruikers. De inactieve klanten worden ook meegenomen in zoekopdrachten. Het is wel mogelijk om data te maskeren, dit wordt wel bij overledenen gedaan. Persoonsgegevens worden na het verstrijken van de wettelijke bewaartermijn niet verwijderd. Als gevolg daarvan ontbreekt de wettelijke grondslag voor het verwerken van persoonsgegevens na het verstrijken van de bewaartermijn. Daarnaast blijven klanten voor alle gebruikers zichtbaar, terwijl dit niet noodzakelijk is.
Risico	Het risico bestaat dat persoonsgegevens na de bewaartermijn nog worden bewaard door UWV WERKbedrijf; dit is onrechtmatig. Ook neemt de impact van een datalek toe wanneer onrechtmatig verwerkte persoonsgegevens worden gelekt.
Aanbeveling(en)	Wij adviseren: 1 Korte termijn: maskeer persoonsgegevens van inactieve klanten, met name de gegevens waarvoor geen wettelijke bewaarplicht geldt en persoonsgegevens van gevoelige aard in vrije tekstvelden. 2 Lange termijn: implementeer een proces of technische maatregel om persoonsgegevens, na het verstrijken van de wettelijke bewaartermijn, te verwijderen en de data van inactieve klanten te maskeren. 3 Daarnaast ondersteunen wij het voornemen van UWV WERKbedrijf om een archiveringssysteem te gebruiken voor de documenten (ongestructureerde data) die zich nu in SONAR bevinden. Tevens is het voor de lange termijn aan te bevelen om ook klantgegevens (gestructureerde data) over te brengen naar een archiveringssysteem.

Bevinding 5.8 – Lokale opslag van SONAR-data	Hoog
Beschrijving	Wij hebben geobserveerd dat medewerkers van een regiokantoor exportlijsten van SONAR lokaal opslaan en niet verwijderen. In de mappen bevinden zich nog exportlijsten van 2019 en 2018. Deze bevatten nog BSN en NAW-gegevens. Er zijn recentelijk instructies gekomen hoe om te gaan met het lokaal opslaan van deze exportlijsten, maar hier vindt nog geen monitoring op plaats.
Risico	Het risico bestaat dat persoonsgegevens na de wettelijke bewaartermijn niet verwijderd worden. Daarnaast blijft het risico bestaan dat een datalek zich voordoet met oude bestanden inclusief BSN en NAW-gegevens. Dit kan leiden tot boetes door de AP en reputatieschade.
Aanbeveling(en)	Wij adviseren: 1 Instrueer medewerkers over de wijze waarop exportlijsten en bestanden vanuit SONAR tijdelijk lokaal opgeslagen mogen worden, en monitor dit proces. Zorg er daarnaast voor dat gedeelde schijven (automatisch en) periodiek worden gescand en geschoond, bijvoorbeeld met behulp van tooling.

[redacted]

Art. 10 lid 2 sub e en g Wob

6. Policies

Betreft de informatievoorziening naar betrokkenen over hun gegevensverwerkingen, en naar medewerkers over hoe zij persoonsgegevens mogen verzamelen, gebruiken, bewaren, delen en verwijderen.

INITIEEL	HERHAALBAAR	GEDEFINIEERD	GEMANAGED	GEOPTIMALISEERD

Context

Interne policies

Ieder product, iedere dienst en ieder proces van UWV WERKbedrijf is omschreven in QRC-handleidingen, waarin ook het gebruik in SONAR is vastgelegd. Aanvullend op de functionele handleiding, zijn er voor de gegevensbescherming gouden regels en gedragscodes opgesteld die vastleggen hoe medewerkers persoonsgegevens mogen verzamelen, gebruiken, bewaren, delen en verwijderen.

Externe policies

Er is een privacybeleid op WERK.nl gepubliceerd, conform de vereisten van artikel 13 AVG. Met betrekking tot SONAR ontbreken hier echter enkele belangrijke details.

Bevindingen

6.1	Privacy statement WERK.nl reflecteert niet accuraat de verwerkingen in SONAR	Hoog

Bevinding 6.1 – Privacy statement WERK.nl reflecteert niet accuraat de verwerkingen in SONAR	Hoog
Beschrijving	Het kopje "Ondersteuning bij het vinden van werk" in het privacy statement op WERK.nl is met name relevant met betrekking tot SONAR. Wij hebben gesignaleerd dat belangrijke details ontbreken, zoals gevoelige categorieën persoonsgegevens als de sociale context, het BSN-nummer, en dat het cv gedeeld kan worden met commerciële uitzendbureaus.
Risico	Het risico is dat niet voldaan wordt aan het transparantiebeginsel van art. 5 AVG. Voor het vertrouwen in de overheid is het belangrijk dat burgers juist worden geïnformeerd over de verwerking van hun gegevens.
Aanbeveling(en)	Wij adviseren: 1 Zorg voor een proces, mogelijk tezamen met het updaten van het register van verwerkingsactiviteiten onder 2, waarin er meer koppeling is tussen verwerkingen in belangrijke applicaties, en het privacy statement. 2 Zorg ervoor dat het privacy statement in ieder geval alle bijzondere en gevoelige persoonsgegevens en verwerkingen bevat.

7. Processes, Procedures & Technology

Privacyspecifieke processen, procedures en de ondersteunende technologie die nodig zijn om ervoor te zorgen dat de organisatie persoonsgegevens verwerkt in overeenstemming met haar verplichtingen.				
INITIEEL	HERHAALBAAR	GEDEFINIEERD	GEMANAGED	GEOPTIMALISEERD

Context

Alle nieuwe processen moeten langs de intekentafel, waar IB&P ook altijd aanwezig is. Daarnaast is er een proces voor het afhandelen van inzage- en correctieverzoeken. Deze worden in de meeste gevallen regionaal afgehandeld. Verwijderverzoeken worden altijd in samenwerking met IB&P afgehandeld. Hoewel wel enkele GEB's of soortgelijke risicobeoordelingen zijn gedaan, is er geen volledig beeld over SONAR-risico's gevormd, terwijl de AVG al bijna twee jaar van kracht is.

Bevindingen		
7.1	De risico's met betrekking tot SONAR zijn niet volledig vastgelegd/geïdentificeerd in GEB's	Midden
7.2	Er is geen overzicht van verzoeken van rechten van betrokkenen, omdat aanvragen via het regiokantoor worden afgehandeld. Daarnaast is er geen procedure voor het tijdig en correct afhandelen van deze verzoeken	Laag

Bevinding 7.1 – De risico's met betrekking tot SONAR zijn niet vastgelegd/geïdentificeerd in een GEB	Midden
Beschrijving	De GEB's zijn de methodologie om risico's van nieuwe processen en verandersignalen te beoordelen. Voor de bestaande processen heeft het BG vastgesteld dat een gap-analyse gedaan moet worden. Hoewel enkele GEB's of soortgelijk zijn uitgevoerd voor SONAR of processen die betrekkingen hebben op SONAR, is twee jaar na inwerkingtreding van de AVG nog geen GEB (of privacy impact assessment) uitgevoerd op SONAR als geheel die een volledig beeld geeft van de verwerkingsrisico's.
Risico	Door het ontbreken van een GEB op (één van de meest kritieke) systemen of processen van UWV WERKbedrijf, is er geen overzicht van de risico's voor SONAR en worden deze niet (of onvoldoende) beoordeeld en gemitigeerd.
Aanbeveling(en)	Wij adviseren: 1 Richt een risicomanagementproces in voor SONAR waarbij alle risico's stelselmatig worden geïndiceerd, geclassificeerd, beoordeeld en opgevolgd met bijbehorende processen voor risicoclassificatie en opvolging.

Bevinding 7.2 – Er is geen overzicht en eenduidige procedure voor het afhandelen van verzoeken van rechten van betrokkenen	Laag
Beschrijving	Afhandeling van verzoeken van rechten van betrokkenen gebeurt regionaal. Verwijderverzoeken worden altijd in samenwerking met IB&P afgehandeld. Er is geen centraal overzicht van de hoeveelheid verzoeken die worden ingediend, wanneer deze worden ingediend en of ze zijn afgehandeld. Daarnaast hebben wij niet vast kunnen stellen dat er een checklist is voor het afhandelen van verwijderverzoeken, waarin wordt aangegeven waar (in welke systemen en ongestructureerde data in mappen) persoonsgegevens verwijderd dienen te worden om te waarborgen dat alle verzoeken correct en tijdig worden afgehandeld. Er vindt ook geen steekproefsgewijze controle plaats voor het correct en tijdig afhandelen van verzoeken van betrokkenen.
Risico	Het risico bestaat dat sommige persoonsgegevens niet worden verstrekt of verwijderd bij inzage- en verwijderverzoeken. Daarnaast bestaat het risico bij regionaal opvolgen zonder checklist dat managers in de regio de persoonsgegevens waarvan ze weten dat UWV WERKbedrijf deze verwerkt, verstrekt of inzichtelijk maakt, maar niet de persoonsgegevens die zich ergens anders binnen de organisatie bevinden. Daarmee wordt niet voldaan aan de AVG om alle persoonsgegevens te verstrekken of te verwijderen. Dit kan leiden tot boetes door de AP.
Aanbeveling(en)	Wij adviseren: 1 Creëer en beheer een centraal overzicht van alle verzoeken inclusief status van afhandeling en de datum van indiening en opvolging. Om de correctheid van afhandeling te waarborgen, is het aan te raden om te faciliteren dat verzoeken via centrale kanalen ingediend en afgehandeld worden. 2 Stel daarnaast een checklist op van hoe en in welke systemen persoonsgegevens verwijderd of overhandigd kunnen worden.

8. Security for Privacy

De mate waarin persoonsgegevens adequaat beveiligd zijn, waarbij rekening wordt gehouden met de ernst en de waarschijnlijkheid van een privacy-inbreuk.				
INITIEEL	HERHAALBAAR	GEDEFINIEERD	GEMANAGED	GEOPTIMALISEERD

Context

Wij zijn geïnformeerd dat er verschillende maatregelen getroffen zijn om persoonsgegevens in SONAR te beschermen. Zo worden pentests uitgevoerd op SONAR, mutaties gelogd, gemonitord door [redacted] en heeft SONAR als KPI SSD-compliant te worden. De informatiebeveiliging zal nader onderzocht worden in het deelonderzoek Informatiebeveiliging. Hieronder zijn de eerste bevindingen hieromtrent genoteerd.

Art. 10 lid 2 sub g Wob

Bevindingen

8.1	Toegangsrechten zijn niet beperkt op basis van 'need-to-know'-principe	Hoog
[redacted]		

Art. 10 lid 2 sub e en g Wob

Bevinding 8.1 – Toegangsrechten zijn niet beperkt op basis van 'need-to-know'-principe	Hoog
Beschrijving	Toegangsrechten zijn niet beperkt op basis van het 'need-to-know'-principe. Zie de details hiervan onder hoofdstuk 5. Data Lifecycle Management.
Risico	[redacted]
Aanbeveling(en)	Het deelonderzoek met betrekking tot IAM zal specifieke aanbevelingen bevatten over het verbeteren van het toegangsmanagement.

Art. 10 lid 2 sub e en g Wob

[redacted]

Art. 10 lid 2 sub e en g Wob

[redacted]

Art. 10 lid 2 sub e en g Wob

[redacted]

Art. 10 lid 2 sub e en g Wob

9. Third Party Management

Processen die beheren hoe derden de persoonsgegevens beschermen namens een organisatie.				
INITIEEL	HERHAALBAAR	GEDEFINIEERD	GEMANAGED	GEOPTIMALISEERD

Context

De softwareontwikkelaar van SONAR is [redacted]. Deze is ISO 27001 gecertificeerd. De hostingpartij voor SONAR is [redacted]

Art. 10 lid 2 sub g Wob

Bevindingen		
9.1	Er is onvoldoende ontwikkelcapaciteit bij de softwareontwikkelaar en verder in de markt om te voldoen aan de eisen die UWV WERKbedrijf aan SONAR stelt met betrekking tot privacy	Midden

Bevinding 9.1 – Er is onvoldoende ontwikkelcapaciteit bij de softwareontwikkelaar om te voldoen aan de eisen die UWV WERKbedrijf aan SONAR stelt met betrekking tot privacy	Midden
Beschrijving	Uit documentatie blijkt dat SONAR (en Siebel) veel maatwerk behoeft. SONAR bestaat voor 50% uit maatwerk. In de markt is onvoldoende ontwikkelcapaciteit beschikbaar, omdat Siebel-ontwikkelaars schaars zijn. Het doorvoeren van functionele wijzigingen is beperkt mogelijk. Daarnaast is het binnen de huidige inrichting van SONAR niet mogelijk om per rol en medewerker gegevens af te schermen en bulkverwerking uit te voeren. [redacted] Op dit moment liggen de kosten voor SONAR en VerA tussen de EUR 12 en 13 miljoen per jaar voor onderhoud, beheer en datacentrum.
Risico	Het risico bestaat dat onderhoudskosten op termijn niet meer in verhouding staan tot de waarde die het systeem biedt, gezien de schaarste in de markt met betrekking tot ontwikkelcapaciteit.
Aanbeveling(en)	Wij adviseren: 1 Houd rekening bij het kiezen van een nieuwe leverancier met de expertise op het gebied van privacy by design.

Art. 10 lid 2 sub e en g Wob

10. Training & Awareness

Algemene en specifieke trainingen met betrekking tot het verzamelen, gebruiken, bewaren, vrijgeven en weggooien van persoonlijke informatie van de organisatie en het doorlopende bewustmakingsprogramma om de kennis van privacy te behouden en het belang van privacybescherming aan de medewerkers over te brengen.				
INITIEEL	HERHAALBAAR	GEDEFINIEERD	GEMANAGED	GEOPTIMALISEERD

Context

UWV WERKbedrijf heeft activiteiten ondernomen om de awareness omtrent privacy bij de medewerkers te verhogen. Zo heeft (in ieder geval) de afdeling WSP een online training "veilig omgaan met informatie" moeten volgen. Daarnaast zijn er gouden regels (privacy poster) en is er een Gedragscode. Bovendien was er een e-learning die verplicht was voor alle managers, die nu is omgezet naar een verplichting voor alle UWV-medewerkers. Ook op het intranet van UWV is informatie te vinden over privacy. Wij hebben geobserveerd dat adviseurs die op dagelijkse basis met meer gevoelige gegevens werken meer privacybewustzijn hebben, en weten wat ze mogen noteren in SONAR.

Bevindingen		
10.1	Sommige medewerkers gebruiken 'workarounds' omdat ze het privacyrisico niet begrijpen	Hoog
10.2	De effectiviteit van trainingen wordt niet getoetst	Midden

Bevinding 10.1 – Sommige medewerkers gebruiken 'workarounds' omdat ze het privacyrisico niet begrijpen	Hoog
Beschrijving	Medewerkers gebruiken 'workarounds' omdat ze het privacyrisico niet voldoende begrijpen. Wij hebben geobserveerd dat medewerkers van een regiokantoor met een workaround werken om persoonsgegevens zoals het BSN toe te voegen aan de exports vanuit SONAR, die als privacymaatregel geen BSN-nummer en NAW-gegevens meer bevatten. Daarnaast hebben wij ook geconstateerd dat exports op de harde schijf worden opgeslagen en niet worden verwijderd.
Risico	Het risico is dat men (ten onrechte) het gevoel heeft dat technische maatregelen geïmplementeerd zijn en daarmee de beveiliging van SONAR op orde is, maar dat medewerkers onjuist (blijven) handelen waardoor de genomen maatregelen niet effectief zijn.
Aanbeveling(en)	Wij adviseren: 1 Instrueer medewerkers over de juiste werkwijze en leg daarbij duidelijk uit om welke redenen bepaalde werkwijzen zijn gewijzigd. 2 Controleer regelmatig op de naleving van de nieuwe gedragsregels. 3 Instrueer medewerkers die toegang hebben tot de dashboards over het lokaal opslaan en verwijderen van exports. Een mogelijkheid is om een (of meerdere) centrale mappen te beheren die na 24 uur automatisch geschoond worden. Hierbij is ook een rol weggelegd voor de (operationeel) manager.

Bevinding 10.2 – De effectiviteit van trainingen wordt niet getoetst	Midden
Beschrijving	Er zijn activiteiten ondernomen voor training en awareness. Echter, de effectiviteit hiervan wordt niet getoetst. Met name wordt het risico/belang van veilig omgaan met persoonsgegevens niet herkend. Als gevolg hiervan gebruiken medewerkers workarounds.
Risico	Het risico is dat medewerkers niet handelen op basis van de privacyregels en daardoor datalekken kunnen veroorzaken.
Aanbeveling(en)	Wij adviseren: 1 Instrueer medewerkers over de juiste werkwijze en leg daarbij duidelijk uit om welke redenen bepaalde werkwijzen zijn gewijzigd. 2 Controleer tevens regelmatig op de naleving van de nieuwe gedragsregels.

11. Monitoring

Het proces om te toetsen of de maatregelen effectief zijn, bijvoorbeeld door middel van self-assessments, interne review of externe audits.				
INITIEEL	HERHAALBAAR	GEDEFINIEERD	GEMANAGED	GEOPTIMALISEERD

Context

Voor regiokantoren is er een jaarlijkse self-assessment waarin bedrijfscontinuïteit en enkele privacy controls worden getoetst door de vestigingsmanager. Ad hoc worden interne onderzoeken geïnitieerd.

Bevindingen

11.1	Er is geen actieve monitoring om te controleren of voorgenomen privacyverhogende maatregelen in SONAR doorgevoerd zijn	Hoog
11.2	Privacymaatregelen worden niet structureel getoetst op effectiviteit	Midden

Bevinding 11.1 – Er is geen actieve monitoring om te controleren of voorgenomen privacyverhogende development changes daadwerkelijk doorgevoerd zijn	Hoog
Beschrijving	Voorgenomen privacymaatregelen die meegenomen moeten worden in de development changes van SONAR worden soms laag geprioriteerd, en daardoor niet uitgevoerd, bijvoorbeeld de schoning van SONAR-data. Op het laag prioriteren, en daarmee niet implementeren van maatregelen, wordt niet proactief en structureel gemonitord noch wordt erover gerapporteerd.
Risico	Het risico is dat functionele wijzigingen voorrang krijgen boven changes die nodig zijn om privacy compliant te worden, zonder dat hier een bewuste risicoafweging over is gemaakt.
Aanbeveling(en)	Wij adviseren: 1 Creëer periodieke overlegstructuur en rapportage tussen PO en IB&P. 2 Zorg er hierbij voor dat er ook een duidelijke escalatielijn is wanneer hoge privacyrisico's niet gemitigeerd (dreigen te) worden.

Bevinding 11.2 – Privacymaatregelen worden niet structureel getoetst op effectiviteit	Midden
Beschrijving	Een recent geïmplementeerde maatregel is dat exports met het BSN vanuit SONAR niet meer mogelijk zijn. Er wordt echter niet structureel gecontroleerd of deze maatregel het beoogde doel bereikt.
Risico	Het risico is dat workarounds worden verzonnen om de technische maatregel te omzeilen.
Aanbeveling(en)	Wij adviseren: 1 Soms komt het voor dat een technische maatregel workarounds in de hand werkt. Controleer daarom of de wijziging, zoals het beperken van de exportfunctionaliteit, ook effectief is. Beoordeel of aanvullende organisatorische maatregelen vereist zijn.

12. Incident Management

De procedure voor het identificeren, beoordelen en reageren op incidenten, inclusief mechanismen en processen voor het uitvoeren van oorzakenanalyse en het treffen van corrigerende acties.				
INITIEEL	HERHAALBAAR	GEDEFINIEERD	GEMANAGED	GEOPTIMALISEERD

Context

UWV beheert een overzicht van het totaal overzicht datalekken en heeft een proces om datalekken te melden. UWV rapporteert meldplichtige datalekken bij de AP. Tevens zijn er corrigerende maatregelen getroffen om de omvang van de schade door datalekken in de toekomst te beperken door het verwijderen van BSN en NAW-gegevens uit de exportlijsten via de BI-dashboards.

Bevindingen		
12.1	Medewerkers hebben onvoldoende kennis over datalekken	Hoog
12.2	Datalekken worden onvoldoende geëvalueerd om in de toekomst te worden voorkomen	Hoog

Bevinding 12.1 – Medewerkers hebben onvoldoende kennis over datalekken	Hoog
Beschrijving	Sommige medewerkers hebben onvoldoende kennis hebben over privacy en hun individuele privacyverantwoordelijkheden. Wij hebben geobserveerd dat sommige medewerkers van een regiokantoor niet of niet voldoende op de hoogte waren van de juiste procedures rondom datalekken. Ook konden ze niet vertellen wat een datalek kwalificeert. Daarnaast worden workarounds verzonnen om de getroffen maatregelen te omzeilen, omdat het privacybelang niet wordt herkend.
Risico	Het risico is dat privacy-incidenten zoals datalekken plaatsvinden en mogelijk niet (of niet op tijd) worden opgemerkt en gerapporteerd.
Aanbeveling(en)	Wij adviseren: 1 Instrueer medewerkers over de juiste werkwijze en leg daarbij duidelijk uit om welke redenen bepaalde werkwijzen zijn gewijzigd. 2 Controleer regelmatig op de naleving van de nieuwe gedragsregels. Communiceer periodiek over datalekken en zorg ervoor dat medewerkers regelmatig een training volgen.

Bevinding 12.2 – Datalekken worden onvoldoende geëvalueerd om in de toekomst te worden voorkomen	Hoog
Beschrijving	Datalekken worden onvoldoende geëvalueerd om in de toekomst te worden voorkomen. Zo wordt geen actieplan gemaakt en uitgevoerd. Zowel uit documentatie als op basis van gesprekken is gebleken dat technische maatregelen naar aanleiding van een datalek niet altijd hoog geprioriteerd worden en daardoor niet geïmplementeerd worden.
Risico	Het risico bestaat dat meer datalekken voorkomen door dezelfde oorzaak. Mogelijk kan de AP een last onder dwangsom opleggen of als ultieme maatregel een (tijdelijk) verwerkingsverbod.
Aanbeveling(en)	Wij adviseren: 1 Zorg ervoor dat na een (groot) privacy-incident een evaluatie wordt uitgevoerd, een actieplan wordt opgesteld en ook wordt uitgevoerd. 2 Beoordeel daarnaast periodiek aan de hand van de incidenten of er verbeteringen mogelijk zijn op basis van de incidentele oorzaak, patronen, veranderingen in wetgeving en de resultaten van de periodieke evaluatie en controleer of de voortgang van verbeteringen is gerapporteerd en beoordeeld door management.

B: Lijst van geïnterviewde personen

Onderstaand hebben wij een overzicht opgenomen van de mensen die wij hebben geïnterviewd als onderdeel van ons onderzoek:

#	Functie
[redacted]	

Art. 10 lid 2 sub e Wob

#	Functie
[redacted]	

Tabel 3 Lijst van geïnterviewden