

Het gebruik van het RRA brengt voor het Instituut een aantal risico's of aandachtspunten met zich mee. Hieronder volgt een opsomming van de risico's die deels ook door de DPIA benadrukt worden:

- 1) Betrokken partijen:** In de DPIA wordt veelvuldig gerefereerd aan SAP HR vanwaar de persoonsgegevens geïmporteerd worden in de RRA. Wanneer persoonsgegevens vanuit SAP HR verstrekt worden aan de RRA, dan zal SAP HR onderdeel vormen van de gegevensverwerkingen die plaatsvinden met betrekking tot de RRA. De applicatie van SAP HR wordt door het Instituut beheerd, maar de ontwikkelaar is SAP. Hierom zal ook deze partij als betrokken partij moeten worden opgenomen in hoofdstuk vijf van de DPIA. SAP is in deze gegevensverwerkingen aan te merken als verstrekker en verwerker.
- 2) Onduidelijke gegevensverwerkingen en doeleinden:** In hoofdstuk drie van de DPIA wordt in detail ingegaan op het proces van de RRA. Hiervan is ook een overzichtelijk schema toegevoegd. Het doel van hoofdstuk drie ziet echter niet alleen op het in kaart brengen van het proces, maar ook op welke specifieke gegevensverwerkingen plaatsvinden waarbij duidelijk de categorieën persoonsgegevens verbonden worden aan de gegevensverwerking. In hoofdstuk drie wordt niet ingegaan op de categorieën persoonsgegevens noch wordt duidelijk gemaakt in een tabel (zoals wel is opgenomen in het Rijksmodel DPIA) welke categorieën persoonsgegevens behoren aan welke gegevensverwerking. Doordat de gegevensverwerkingen met persoonsgegevens niet goed in beeld zijn gebracht, kan er nu niet juist beoordeeld worden of bij elke gegevensverwerking aan het principe van data-minimalisatie voldaan wordt.

Verder wordt in hoofdstuk acht van de DPIA het SAP Business Technology Platform (hierna: "SAP BTP") en het SAP Human Capital Management (hierna: "SAP HCM") benoemd. In de beschrijving hierover wordt gesproken over het uitwisselen van de gegevens uit de RRA middels een API naar het SAP BTP of SAP HCM. Hierover wordt echter geen uitleg gegeven over welke gegevens uitgewisseld worden met het SAP BTP, of hier sprake is van persoonsgegevens, voor welk doeleinde de gegevens gebruikt worden en of het Instituut hier ook gebruik van maakt. Indien hier persoonsgegevens worden uitgewisseld, dan zal dit ook als gegevensverwerking benoemd moeten worden. Bij SAP HCM worden wel persoonsgegevens gedeeld uit de RRA, echter blijft het onduidelijk in hoofdstuk twee of drie welke persoonsgegevens hier uitgewisseld worden.

In hoofdstuk elf wordt de rechtmatigheid van de gegevensverwerking beoordeeld. Opvallend is dat hier maar één gegevensverwerking wordt weergegeven, terwijl in hoofdstuk drie over de gegevensverwerkingen juist in ieder geval elf verschillende soorten gegevensverwerkingen worden opgesomd. Indien zoveel gegevensverwerkingen in het proces worden vastgesteld, dan zullen deze gegevensverwerkingen ook moeten worden opgesomd in hoofdstuk elf voor de beoordeling van de rechtsgrond. Door het weglaten van deze gegevensverwerkingen is het nu onduidelijk of er een grondslag bestaat voor alle gegevensverwerkingen, waardoor sommige gegevensverwerkingen van het proces als onrechtmatig beschouwd kunnen worden.

- 3) Beveiliging:** In hoofdstuk vier van de DPIA wordt ingegaan op de technische en organisatorische maatregelen. Hier wordt benoemd dat de persoonsgegevens in de RRA behandeld worden op het niveau van BBN2 en dat hier strikte voorwaarden aan verbonden zijn. De keuze voor het niveau van BBN2 wordt echter niet onderbouwd waardoor onduidelijk is waarom voor dit niveau gekozen is. Daarnaast worden de individuele beveiligingsmaatregelen vanuit de Baseline informatiebeveiliging Overheid (hierna: "BIO") niet in de DPIA opgenoemd en beargumenteerd hoe de beveiligingsmaatregelen in de RRA voldoen aan de opgestelde normen in de BIO. Door deze onduidelijkheid kan niet goed beoordeeld worden of de RRA de juiste beveiligingsmaatregelen heeft genomen om de persoonsgegevens adequaat te beveiligen.
- 4) Geautomatiseerde besluitvorming:** In de DPIA wordt aangegeven dat er sprake is van geautomatiseerde besluitvorming. Aan de hand van het rooster kunnen vervolgens de

juiste toelagen en vergoedingen op basis van CAO- en ATW-regels bepaald worden. Uit de DPIA blijkt dat deze gegevens niet door het Instituut verwerkt worden, terwijl de DPIA aangeeft dat deze mogelijkheid wel in de RRA is opgenomen. De DPIA geeft niet weer waarom hier sprake is van geautomatiseerde besluitvorming aan de hand van artikel 22 lid 1 AVG en voor welke grondslag voor de ingebruikname van een dergelijke geautomatiseerde besluitvorming uit artikel 22 lid 2 AVG gekozen is. Alhoewel op dit moment door het Instituut geen gebruik gemaakt gaat worden van de functionaliteit om de toelagen en vergoedingen automatisch te laten bepalen, zal wel onderbouwd moeten worden of hier in de toekomst wel gebruik gemaakt van gaat worden en hoe deze geautomatiseerde besluitvorming zich verhoudt tegen artikel 22 AVG.

- 5) Bewaartermijnen:** De bewaartermijnen in hoofdstuk tien van de DPIA zijn op categorie persoonsgegevens weergegeven. Door deze wijze kan niet per gegevensverwerking beoordeeld worden over hoelang persoonsgegevens bewaard blijven bij een gegevensverwerking. Voor verschillende gegevensverwerkingen kunnen namelijk verschillende bewaartermijnen gelden terwijl de categorieën persoonsgegevens in die gegevensverwerkingen hetzelfde zijn. Hierdoor zal het huidige overzicht in de DPIA niet het gewenste effect hebben om effectief te kunnen handhaven op de bewaartermijnen. Het is gebruikelijk dat de bewaartermijnen per gegevensverwerking worden weergegeven waar vervolgens ook de betreffende categorieën persoonsgegevens worden weergegeven.

Overige aandachtspunten

- 1) Verschillende termen voor verwerkingsverantwoordelijke:** In de gehele DPIA wordt gebruik gemaakt van verschillende termen die hetzelfde aanduiden. Voor "gebruikersorganisatie" wordt namelijk ook "eindgebruiker" of "beheerder" gebruikt. Door deze verschillende aanduidingen ontstaat er verwarring met betrekking tot welke partij wordt aangeduid.
- 2) Technische en organisatorische maatregelen op de verkeerde plek:** In hoofdstuk zestien en zeventien van de DPIA worden technische en organisatorische maatregelen benoemd die al van toepassing zijn. De locatie voor deze informatie is echter niet juist aangezien deze technische en organisatorische maatregelen al onderdeel uitmaken van het proces. Hierom is het aan te raden om deze informatie al op te nemen in hoofdstuk acht zodat hier een duidelijk overzicht aanwezig is van de technische en organisatorische maatregelen.

Conclusie

Doordat de RRA in gebruik genomen wordt, zal het Instituut efficiënter kunnen roosteren met betrekking tot de zaakbegeleiders en facilitaire medewerkers. Hierdoor wordt een sluitende operationele planning gemaakt voor buiten de kantooruren. De ingebruikname van de RRA brengt echter wel risico's met zich mee. Veel van de risico's zijn in de DPIA opgenomen en er zijn ook maatregelen voorgesteld die voornamelijk op de RRA zien, maar niet zozeer op de organisatie.

Zoals in de aanleiding benoemd is, is het opstellen van een DPIA voor het Instituut waarschijnlijk niet verplicht. Het Ministerie heeft echter wel een DPIA opgesteld over de interne werking van de RRA en heeft hierin de risico's opgenomen en de juiste maatregelen voorgeschreven voor de RRA. Deze DPIA is hierdoor van algemene aard, maar is niet geheel kloppend. De onduidelijkheid over de gegevensverwerkingen, welke persoonsgegevens per gegevensverwerking verwerkt worden en welke doeleinden behoren bij welke gegevensverwerking speelt hierbij een grote rol. Dit had nader gespecificeerd moeten worden of waar mogelijk had de eindgebruiker, zoals het Instituut, gevraagd moeten worden om hierop aanvullende informatie te geven. Verder zijn de betrokken partijen niet allemaal opgenomen, is de onderbouwing van de beveiliging niet voldoende en worden de bewaartermijnen niet aan de gegevensverwerkingen verbonden. Ook de grondslagen voor de gegevensverwerkingen is voor maar één verwerking opgenomen, terwijl er aangegeven wordt dat er sprake is van meerdere gegevensverwerkingen.

De oplegger van het Instituut geeft toevoegende informatie over hoe de DPIA zich verhoudt tot de implementatie bij de RRA. Het Instituut geeft nu nog niet kenbaar hoe met automatische besluitvorming wordt omgegaan. Daarnaast is het onduidelijk of gebruikers op dit moment worden geïnformeerd over hoe persoonsgegevens in de RRA gebruikt mogen worden.

Advies

Voor de voorgenomen gegevensverwerkingen geef ik een **positief advies**. Door de gegevensverwerkingen die plaatsvinden in de RRA, wordt het proces van roosteren voor de zaakbegeleiders en facilitaire medewerkers geoptimaliseerd. Deze medewerkers worden hierdoor zo effectief mogelijk ingezet binnen het Instituut. De gegevensverwerkingen in de RRA zorgen daarnaast voor het Instituut dat er geen hoog risico is, waardoor het opstellen van een DPIA niet noodzakelijk is geweest. Een hoog risico bestaat hier waarschijnlijk niet voor de betrokkenen.

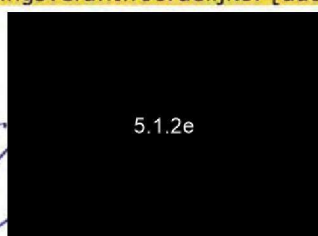
Wel zal het Ministerie de DPIA over de RRA moeten herzien indien mogelijk. Hierin zal het Ministerie een aantal onderwerpen moeten herzien. Ten eerste zullen alle betrokken partijen in het overzicht opgenomen moeten worden. Ten tweede zal er een duidelijk overzicht van de gegevensverwerkingen opgenomen moeten zodat duidelijk wordt welke persoonsgegevens bij een gegevensverwerking verwerkt worden en voor welk specifiek doeleinde de persoonsgegevens verwerkt worden. Ten derde zullen de bewaartermijnen anders geformuleerd moeten worden zodat per gegevensverwerking een bewaartermijn aanwezig is. Ten vierde zal een beter onderbouwing van de gekozen technische en organisatorische maatregelen weergegeven moeten worden. Tot slot zal beter gekeken moeten worden naar welke inhoud waar hoort in de DPIA.

Het Instituut zal ook een aantal maatregelen moeten nemen. Het Instituut zal kenbaar moeten maken of ook gebruik gemaakt gaat worden van de automatische besluitvorming optie in de RRA. Daarnaast zal bewustzijn gecreëerd moeten worden bij de gebruikers van het Instituut ten aanzien van welke persoonsgegevens gebruikt mogen worden in de RRA volgens deze DPIA.

Vaststelling verwerkingsverantwoordelijke: [datum]

Naam:

Siebe Keulen



5.1.2e

20-04-2025



GEGEVENSBE SCHERMINGSEFFECTBEOORDELING RIJKS ROOSTERAPPLICATIE (DPIA RRA)

Versie 1.0

Contact Ministerie van BZK, directie CIO -Rijk

PAR- team: 5.1.2i minbzk.nl

Revisiegegevens

Versie	Datum	Auteur	Omschrijving
	23-06-2023		Eindresultaat initiële versie
0.95	10-10-2023	5.1.2e	Opmerkingen programma- en privacyteam 5.1.2e
		5.1.2e	
		5.1.2e	
1.0	24-10-2023	5.1.2e	Verwerking review commentaar 5.1.2e (Privacy Officer / Security Officer)
		5.1.2e	

Verwijzingen

Verwijzingen vanuit de DPIA naar projectdocumenten.

Document	Versie

Introductie

Dit is de DPIA voor de rijks roosterapplicatie (RRA). In de paragrafen op de navolgende pagina's wordt de gegevensverwerking, -bescherming, de verwerkingsdoeleinden en de belangen van gegevensverwerking uiteengezet voor de RRA.

Deze DPIA is uitgevoerd vanwege het verlopen van het beleidstermijn van 3 jaar van de vorige DPIA (PIA HNR_RIR v2.1), die was uitgevoerd voor het programma "Het Nieuwe Roosteren" (HNR).

Deze DPIA wordt opgenomen in het Beheerdossier RRA, waarbij het in onderhoud komt bij het Centraal Functioneel Beheer van RRA (belegd bij O&P Rijk).

Tijdens het opstellen van de DPIA zijn projectmedewerkers veelvuldig geconsulteerd. Onder andere de volgende functies zijn bij de totstandkoming van deze DPIA betrokken:

- Product Owner RRA
- Privacy Adviseur Rijk
- Business analisten
- Centraal Functioneel Beheer
- Applicatie architect

Er is gebruik gemaakt van het model gegevensbeschermingseffectbeoordeling rijksdienst (DPIA). In hoofdstuk 2 en 3 is aandacht besteed aan standaard verwerkingen die in veel DPIA's afwezig zijn. In hoofdstuk 8 wordt een datastroommodel gebruikt voor het weergeven van de technische inrichting, om zo te compenseren voor de afwezigheid van een architectuurperspectief in de DPIA.

In de risicoanalyse (hoofdstuk 16) is gebruik gemaakt van Soloves taxonomie van privacy en het datastroommodel om risico's te modelleren. Beide methoden hebben geleid tot nieuwe inzichten in de privacyrisico's van RRA. In hoofdstuk 17 zijn per risico meerdere mogelijke maatregelen voorgesteld, waarbij aandacht wordt besteed aan zowel het wegnemen als het mitigeren van risico's.

Met de DPIA 2017 heeft de GOR Rijk ingestemd (Instemmingsverzoek GOR Rijk 17.116). Daarnaast adviseert de GOR om een jaar na invoering van het systeem een evaluatie te houden en hierover te rapporteren

aan de GOR Rijk. Deze DPIA vervangt de DPIA uit 2017. De DPIA uit 2017 is als input gebruikt voor deze hernieuwde versie. En het proces voor het opstellen van deze DPIA is geheel opnieuw doorlopen. Deze DPIA is initieel opgesteld voor dat de verwerking is begonnen om deze nogmaals te toetsen aan de AVG.

Naast de DPIA is voor RRA een Solution Architectuur met daarin beveiligingsmaatregelen opgesteld en wordt een fit-gap BIO uitgevoerd. Dit is ook belegd bij O&P Rijk. Tevens voldoet de oplossing aan de ABDO.

Gebruik van deze DPIA

Deze DPIA bespreekt de scope van de RRA-oplossing zoals beschreven. Organisaties kunnen data uit de RRA (bv door een API koppeling) inzetten voor processen buiten de RRA om. Dit is aan de afnemer om in te richten. Een organisatie kan bijvoorbeeld de RRA gebruiken voor de planning en eigen (aanpalende)processen toevoegen. Wanneer er sprake is van additionele gegevensverwerkingen wordt het opstellen van een aanvullende DPIA voor deze verwerkingen met kruisverwijzingen naar dit document geadviseerd.

Inhoudsopgave

A. Beschrijving kenmerken gegevensverwerkingen 6

- 1. Voorstel 6
 - 1.1 Aanleiding 6
 - 1.2 Toelichting 7
- 2 Persoonsgegevens 8
- 3 Gegevensverwerkingen 10
- 4 Verwerkingsdoeleinden 14
- 5 Betrokken partijen 15
- 6 Belangen bij de gegevensverwerkingen 16
- 7 Verwerkingslocaties 17
- 8 Technieken en methoden van de gegevensverwerkingen 17
- 9 Juridisch en beleidsmatig kader 21
- 10 Bewaartermijnen 21

B. Beoordeling rechtmatigheid gegevensverwerkingen 23

- 11 Rechtsgrond 23
- 12 Bijzondere persoonsgegevens 24
- 13 Doelbinding 24
- 14 Noodzaak en evenredigheid 24
- 15 Rechten van betrokkenen 25

C & D. Beschrijving en beoordeling risico's voor de betrokkenen en maatregelen 26

- 16 Risico's voor betrokkenen en 17 maatregelen 26

E. Bijlagen 30

- E1 Toetsen gerechtvaardigd belang 30

Bijlage 1-DPIA RRA- Grondslag gerechtvaardigd belang 30

- E2 Toets proportionaliteit en subsidiariteit 31

A. Beschrijving kenmerken gegevensverwerkingen

1. Voorstel

Binnen de rijksoverheid wordt door verschillende onderdelen gewerkt in roosterdiensten. Er is op dit moment sprake van verschillen in zowel rechtspositie als in organisatie van het werken in rooster-diensten binnen de overheid. Rijksbreed is sinds 2020 een programma 'Het Nieuwe Roosteren', voorheen 'Rooster Innovatie Rijk' (RIR), actief om een Rijksbreed afgestemde benadering van het werken in roosterdiensten te realiseren. Het programma HNR heeft, na definitieve goedkeuring door het ICBR, O&P Rijk gevraagd een efficiënte centrale dienstverlening en systeemondersteuning te realiseren voor het roosterproces binnen de Rijksoverheid waarvan roosterdiensten desgewenst gebruik kunnen maken. Er zal daarbij sprake zijn van een fasegewijze aansluiting en ontwikkeling. De dienstverlening kent bij de start een beperkt aantal deelnemers en een basale dienstverlening. Fasegewijs zal het aantal deelnemers toenemen en de dienstverlening verder worden uitgebreid.

1.1 Aanleiding

De aanleiding voor de ontwikkeling van de Rijksbrede dienst voor roosteren is het programma HNR. Belangrijk resultaat van dit programma is uniformeren en harmoniseren van roosteren binnen het Rijk. Het programma 'Dienstverlening op ondersteuning Roosterprocessen (DOOR)' is opgezet om invulling te geven aan deze ambitie.

Het programma DOOR realiseert een Rijksbrede dienst voor roosteren bij O&P Rijk die afgenomen kan worden door de roosterende onderdelen van de Rijksoverheid. Deze dienstverlening wordt verwezenlijkt met een applicatie voor de ondersteuning van het plannen en uitvoeren van roosters (onder toetsing van Wet- en Regelgeving zoals de Arbeidstijdenwet (ATW)) voor de inzet van intern en extern personeel. Het systeem berekent op basis van een vastgesteld en gerealiseerd rooster ook de soorten uren(recht op toelagen en vergoedingen) die de uitvoering van het rooster tot gevolg heeft. De gegevens die uit de roosterdienst voortkomen worden gebruikt voor de verloning aan de betrokken medewerkers en voor de communicatie van aan- en afwezigheid aan de HR-administratie.

De Rijksbrede drijfveren voor het implementeren van een centrale Rijksbrede dienst voor roosteren zijn:

- De werkvraag verandert; Duurzaam inzetbaar blijven;
- Tijd-, plaats- en apparaat onafhankelijk werken;
- Meeroosteren (selfservice);
- Professionaliseren roosteren;
- Uniforme verloning conform CAO Rijk;

- Creëren van een eigentijds uniform roosterproces dat de eigenheid van elke uitvoeringsorganisatie binnen het Rijk ondersteunt;
- Op termijn creëren van schaalvoordeel bij ontwikkeling, beheer en digitale procesondersteuning.

1.2 Toelichting

Het roosterstatuut was bedoeld als kader voor een Rijksbreed uniform roosterproces. Dit kader moest ervoor zorgen dat een flexibele, effectieve en efficiënte uitvoering van het werk op Rijksbreed niveau mogelijk is maar er ook ruimte bestaat voor specifieke invulling wanneer de werksituatie daarom vraagt. Een onderdeel van het roosterproces is meeroosteren.

Zowel meeroosteren en traditioneel roosteren, zijn roostervarianten die door de RRA wordt ondersteund. (Mee)roosteren vraagt om een informatie/gegevens van de organisatie (de capaciteitsvraag) enerzijds en medewerkers anderzijds.

Deze DPIA is een actualisatieslag van de eerder opgestelde DPIA.

2 Persoonsgegevens

In de RRA worden de in onderstaande tabel benoemde (categorieën) persoonsgegevens verwerkt. Het uitvragen van de gegevens in de verschillende categorieën kan per organisatie verschillen. (Door organisatie-eigen proces inrichtingen/actoren, rolinrichting en autorisatiebeheer) Dit valt onder de verantwoordelijkheidsgebied van de verwerkingsverantwoordelijke en dient daar in het register van verwerking te worden opgenomen.

Categorie betrokkenen	Categorie persoonsgegevens	Persoonsgegevens	Type persoonsgegevens	Bron	Optioneel *
Medewerker	Identificerende persoonsgegevens	Personeelsnummer, RIN Rijks Identificerend Nummer	Gewoon	SAP HR (P-administratie)	
Medewerker	Identificerende persoonsgegevens	Naam (Voorletters, Voorvoegsel, Tussenvoegsels, Achternaam, ed.)	Gewoon	SAP HR (P-administratie)	
Medewerker	Geslachtgegevens	Geslacht	Gewoon	SAP HR (P-administratie)	Ja **
Medewerker	Adresgegevens	Adres, postcode woonplaats, land	Gewoon	SAP HR (P-administratie)	Ja **
Medewerker	Contactgegevens	Rijks emailadres, Zakelijk telefoonnummer	Gewoon	SAP HR (P-administratie)	
Medewerker	Werk gerelateerde gegevens	Inzet start- en einddatum, functie, afdeling, werktijd, arbeidsduur, Te realiseren uren, 1 ^e en laatste dag arbeidsongeschikt, ed.	Gewoon	SAP HR (P-administratie)	
Medewerker	Rechtspositionele gegevens	Pers/mdw-subgebied, schaal, geboortedatum, wel/geen recht op vergoeding en toelagen(OVW,TOD/WTW/B&B), Verlofrechten en saldo's, ed.)	Gewoon	SAP HR (P-administratie)	
Medewerker	Rooster-gegevens	Meeroosteren ja/nee, 'Geen bezwaar tegen nachtdiensten', Kwalificaties/eigenschappen, ed.	Gewoon	RRA-Werkgever/ Plannings-verantwoordelijke	Naar inzicht afnemer
Medewerker	Rooster-gegevens	Diensttijden, aan- en afwezigheden, Ziek- en hersteld registratie, gepland als(functie), gepland op(plangroep), ed.	Gewoon	RRA-Werkgever/ Plannings-verantwoordelijke	Naar inzicht afnemer
Gebruiker	Toegangs-gegevens	Username wachtwoord, autorisatie	Gewoon	RRA-CFB/Werkgever/ Autorisatie verantwoordelijke	Naar inzicht afnemer

* Alle velden die niet optioneel zijn, worden door HR geleverd mits:

- deze velden van toepassing zijn voor de betreffende medewerker;
- de informatie in HR aanwezig is;

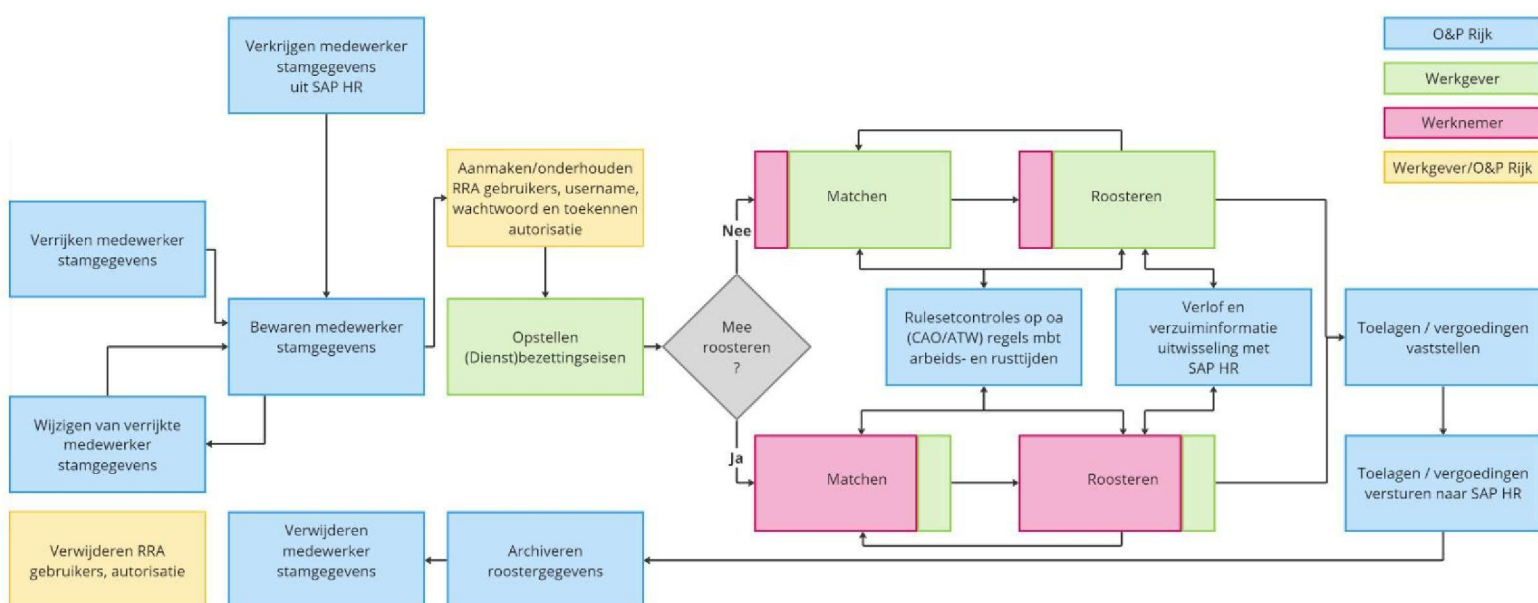
** De gegevensvelden geslachtsaanduiding en/of de adresgegevens zijn standaard niet inbegrepen in de levering van HR aan de RRA. Indien het geslacht en/of de woonadressen bij het roosteren van de medewerkers van belang is, dan kunnen deze gegevens op aangeven van de afnemer worden toegevoegd aan de gegevenslevering vanuit HR.

De persoonsgegevens in de RRA worden via de koppeling met SAP HR ingelezen. Deze gegevens worden gebruikt voor twee doelen

1. Het ondersteunen van het roosterproces zelf
2. Het berekenen van de inconvenienten ten behoeve van de salariering.

De afnemer heeft een invloed op de gegevens die in de RRA worden opgenomen ter ondersteuning van het roosterproces. In deze DPIA worden de gedeelde kenmerken beschreven. Daarnaast zijn er de zogeheten kwalificaties. Dat zijn de afnemer-specifieke persoonskenmerken die in het roosterproces nodig zijn om tot een goed rooster te kunnen komen. Deze DPIA kan niet in algemene zin ingaan op de privacyaspecten die spelen bij kwalificaties die specifiek zijn voor een afnemer. Een afnemer dient hiervoor een in een apart proces een eigen privacy assessment uit te voeren.

Het hoofdproces bij roosteren, weergegeven in onderstaande figuur, gaat uit van de (personele)bezettingseisen. Deze behoeftestelling dient uiteindelijk te leiden tot roosters met voldoende, geschikte aanwezige medewerkers. Niet elk onderdeel van het proces bevat persoonsgegevens, en persoonsgegevens worden ook buiten deze processen in de RRA-oplossing verwerkt. Deze sectie beschrijft de verwerkingen van persoonsgegevens, te beginnen bij het hoofdproces:



Bij de matching worden diensten toegekend aan medewerkers die hiervoor over de juiste kwalificaties beschikken. Dit vormt uiteindelijk de basis voor de roosters. Hierbij wordt rekening gehouden met de contracturen van de medewerker (CAO/ATW) regels mbt arbeids- en rusttijden.

De automatische controles die plaatsvinden in de RRA door middel van 'ruleset' en meldingen die worden gegeven in geval van eventuele overschrijdingen ondersteunen dit proces.

De processtap die is omschreven als roosteren omvat onderdelen als verlof aanvragen, ziek- en hersteld registratie, ruilen- of verschuiven van diensten, inplannen van extra diensten, urenverantwoording. Ter ondersteuning hiervan vindt uitwisseling plaats met SAP HR(O&P Rijk) voor actuele verlof(rechten) en verzuim informatie.

Als een organisatieonderdeel gebruikt maakt van 'meeroosteren' heeft een medewerker een groter aandeel in de processen matchen en roosteren dan het geval is bij 'collectief roosteren'.

De soorten werktijden die volgen uit de processen matchen en roosteren worden in de RRA door de ruleset geëvalueerd en vertaald naar een actuele urenstand en rechten op vergoedingen/toelagen. Deze worden opgestuurd naar SAP HR(O&P Rijk) zodat deze kunnen worden vergoed.

Hieronder staan de relevante processtappen in meer detail beschreven.

Verkrijgen medewerker stamgegevens uit SAP HR

De medewerker stamgegevens ter ondersteuning van het planproces worden voor het overgrote deel geleverd door SAP HR(O&P Rijk) en opgeslagen in de RRA. Hierbij is het aan de afnemer om aan te geven voor welke medewerkers deze gegevens worden geleverd aan de RRA. De afnemer heeft hierbij de keuze of het geslacht en adres onderdeel is van deze gegevenslevering.

Bewaren medewerker stamgegevens

De geleverde medewerker gegevens worden vervolgens opgeslagen in de RRA Medewerker stamdata tabel.

Aanmaken/onderhouden RRA gebruikers, username, wachtwoord en toekennen autorisatie

De Centraal functioneel beheerder (CFB) van O&P Rijk legt één of meerdere Decentraal functioneel beheerders(DFB) aan voor de verschillende afnemers en beheert deze gebruikers. Aan de DFB worden rechten toegekend zodat deze in staat is planners, leidinggevende en andere gebruikers de verdere gewenste rechten toe te kennen en deze te onderhouden.

Verrijken medewerker stamgegevens en wijzigen van verrijkte medewerker stamgegevens

De medewerker stamgegevens die zijn overgekomen uit HR kunnen in de RRA verrijkt worden met verdere gegevens die benodigd zijn voor roosteren. Deze aanvullende informatie is vaak afnemer specifiek en het

toevoegen/onderhouden van deze informatie gebeurd voor het overgrote deel door de afnemer. In uitzonderingssituaties is het mogelijk dat Centraal functioneel Beheer van RRA hier een hand in heeft door het leveren van ondersteuning (in beheer- dan wel implementatie fase van een nieuwe afnemer) Bij het verrijken van gegevens in aanvulling op hetgeen door HR is geleverd kan omvatten:

- Eigenschappen(kwalificaties) van medewerker
 - Deze worden gebruikt om te verduidelijken waar en/of op welke diensten een medewerker inzetbaar is
- Meeroosteren ja/nee
 - Dit wordt gebruikt om te duiden of de medewerker in het planproces meedoet aan meeroosteren en/of voornamelijk de planner/leidinggevende het rooster bepaalt.
- Inzet/plangroep
 - Met dit gegeven wordt aangegeven tot welke roostergroep/locatie een medewerker behoort/ingepland wordt.
- Overige roostergegevens, bijvoorbeeld
 - Ruilgroepen: Dit geeft aan met welke medewerkers/plangroepen medewerkers onderling diensten met elkaar kunnen ruilen;
 - Flexgroepen: Dit geeft aan op welke plangroepen medewerkers flexibel ingezet kunnen worden
 - 'Geen bezwaar tegen nachtdiensten'(voor medewerkers die ouder dan 54 jaar zijn om aan te geven dat zij nog wel/niet nachtdiensten lopen)

Opstellen (Dienst)bezettingseisen

In het hoofdproces stelt de werkgever een (dienst)bezettingseis op. Hiermee wordt op dag-niveau vastgesteld waar, welke - en hoeveel diensten er ingepland moeten worden en over welke kwalificaties een medewerker dient te beschikken om deze diensten te kunnen lopen.

Matchen

Bij de matching worden diensten toegekend aan medewerkers die hiervoor over de juiste kwalificaties beschikken. Dit vormt uiteindelijk de basis voor de roosters. Hierbij wordt rekening gehouden met de contracturen van de medewerker (CAO/ATW) regels met betrekking tot arbeids- en rusttijden. Dit proces wordt ondersteunt door:

- Automatische controles die plaatsvinden in de RRA door middel van de 'ruleset' en meldingen die worden gegeven in geval van eventuele CAO/ATW overschrijdingen en/of onvoldoende verlofsaldo's

- Automatische controles in de applicatie(RRA) en meldingen die worden gegeven in geval van het toekennen waarvoor de medewerker niet beschikt over de juiste eigenschappen(kwalificaties)

Roosteren

Deze processtap omvat onderdelen als verlof aanvragen, ziek- en hersteld registratie, ruilen- of verschuiven van diensten, inplannen van extra diensten en urenverantwoording. Met als doel om te voldoen aan de benodigde capaciteit (bezettingseisen) voor het uitvoeren van werkzaamheden binnen de organisatie. Deze onderdelen kunnen worden uitgevoerd via een web-browser of via de mobiele app.

Verlof en verzuiminformatie uitwisseling met SAP HR

Ter ondersteuning van het roosterproces vindt uitwisseling plaats met SAP HR(O&P Rijk) voor actuele verlof(rechten) en verzuim informatie.

Toelagen / vergoedingen vaststellen en versturen naar SAP HR

Binnen de RRA zijn er verschillende soorten toelagen die toegepast kunnen worden op gewerkte diensten. Zoals TOD, WTV en B&B. De RRA berekend automatisch hoeveel recht een medewerker heeft op deze toelagen.

De soorten werktijden die volgen uit de processen matchen en roosteren worden in de RRA door de ruleset geëvalueerd en vertaald naar een actuele urenstand en rechten op vergoedingen/toelagen. Deze worden opgestuurd naar SAP HR(O&P Rijk) zodat daar de juiste verloning toegepast kan worden.

Archiveren Roostergegevens

Indien een medewerker niet meer geroosterd hoeft te worden zullen de roostergegevens gearchiveerd worden na de vastgestelde termijn. Het doel van het archiveren van deze gegevens is dat de gegevens niet meer actief zichtbaar zijn of gewijzigd kunnen worden binnen de RRA. Maar nog wel inzichtelijk zijn binnen de vastgestelde termijn. Zodat er nog, als dat nodig is, controles uitgevoerd kunnen worden achteraf.

Verwijderen medewerker stamgegevens

Indien een medewerker niet meer ingeroosterd hoeft te worden, dan zullen zijn of haar gegevens na de vastgestelde periode worden verwijderd. Het doel van het verwijderen van de stamgegevens is om te voorkomen dat gegevens onterecht en te lang worden bewaard.

Verwijderen RRA gebruikers, autorisatie

De Centraal functioneel beheerder (CFB) van O&P Rijk verwijdert Decentraal functioneel beheerders(DFB) gebruikers wanneer zij gaan toegang in de RRA meer nodig hebben. De DFB verwijdert gebruikers/autorisatie voor gebruikers waarvan toegang in de RRA aangepast moet worden of niet langer nodig is.

4 Verwerkingsdoeleinden

De RRA ondersteunt het inplannen van roosterpersoneel bij dienstonderdelen van de Rijksoverheid zodat de personele behoefte aan voldoende gekwalificeerd personeel rechtmatig, betrouwbaar, tijdig en op een gebruikersvriendelijke manier wordt ingevuld na een match tussen (beschikbare en gekwalificeerde) medewerkers en gevraagde inzet.

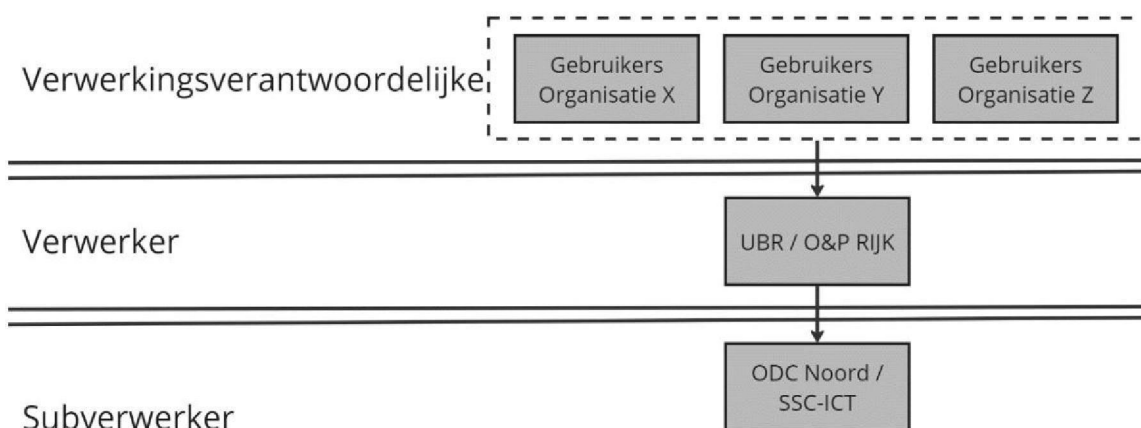
In de RRA worden persoonsgegevens verwerkt voor de volgende doeleinden:

1. Het toekennen van open (nog in te plannen volgens de bezettingseis)diensten aan medewerkers die hiervoor beschikbaar en gekwalificeerd zijn, waardoor uiteindelijk roosters tot stand komen en de juiste bezetting ten behoeve van operationele bedrijfsvoering gewaarborgd is.
2. De juiste toepassing/controles van CAO/ATW werk- en rusttijden regels.
3. Het bepalen van actuele verlofstanden
4. Het voeren van ziek- en hersteld registratie
5. Het bepalen van een actuele urenstand (aantal gewerkte jaaruren) en rechten op vergoedingen/toelagen zodat een juiste verloning toegepast kan worden.

Categorie persoonsgegevens	Doel 1	Doel 2	Doel 3	Doel 4	Doel 5
Identificerende persoonsgegevens	X	X	X	X	X
Adresgegevens	X				
Rechtspositionele gegevens	X	X	X		X
Geslachtgegevens	X				
Werk gerelateerde gegevens	X			X	
Roostergegevens	X	X	X	X	X

5 Betrokken partijen

Vanuit de AVG worden verschillende rollen aangewezen voor organisaties betrokken bij de gegevensverwerkingen in de RRA. De rollen en toepassing zijn hieronder toegelicht en geïllustreerd in onderstaande figuur.



Schematische weergave van AVG-rollen voor betrokken organisaties.

Verwerkingsverantwoordelijke

Organisaties waarbij de RRA gebruikt wordt worden beschreven als afnemers. De medewerkers binnen deze afnemers zijn verantwoordelijk voor de juiste omgang van persoonsgegevens. Binnen afnemers kunnen gebruikers van de RRA specifieke rollen toebedeeld krijgen. Deze rollen zijn bepalend voor welke rechten gebruikers hebben binnen de RRA. Het centrale beheerteam (DCB) stelt de rollen samen en beschikbaar aan afnemers. Het decentrale functionele beheerteam (DFB) vervult de rol als het gaat om toebedelen van rollen aan gebruikers.

Verwerker

O&P Rijk is de organisatie die zorgt voor het aanbieden, onderhouden en (door)ontwikkelen van de RRA. Hieraan liggen verwerkersafspraken ten grondslag.

Geautoriseerde medewerkers binnen O&P Rijk hebben toegang tot de persoonsgegevens binnen de Productieomgeving van de RRA. Deze toegang betreft het ondersteunen van gebruikers en het beheren van de data binnen de RRA.

Vanuit O&P Rijk is er een direct aanspreekpunt voor vragen m.b.t. gegevensverwerking. Datalekken, vragen etc. kunnen geregistreerd worden bij de security office van O&P Rijk. Voor datalekken is de geldende procedure van O&P Rijk en betrokken afnemers van toepassing.

Subverwerker

Voor het technisch beheer van de RRA oplossing wordt samengewerkt met ODC Noord en SSC-ICT. ODC Noord levert de applicatieservers en databases die benodigd zijn om de RRA te ondersteunen.

Naam partij	Rol partij	Functies/afdelingen	Persoonsgegevens
Gebruikers organisatie	Verwerkings-verantwoordelijke	Roosterpersoneel en Decentraal functioneel beheer. Bevoegde medewerkers die roosteren in de RRA	DFB en planner heeft toegang tot bijna alle persoonsgegevens van de eigen medewerkers
O&P Rijk	Verwerker	Bevoegde medewerkers die de RRA onderhouden, DevOps team, Centraal functioneel beheer en Portaal team	Alle persoonsgegevens
Dienstverlener (ODC Noord/ SSC-ICT)	Sub-verwerker	Bevoegde medewerkers vanuit de leverancier die betrokken zijn bij het project. Beheren en onderhouden de applicatieservers en databases.	Geen toegang tot persoonsgegevens

6 Belangen bij de gegevensverwerkingen

Elke partij heeft specifieke belangen bij het verwerken van persoonsgegevens, onderstaande tabel geeft per betrokken partij aan wat het belang is.

Betrokken Partij	Belangen
Gebruikersorganisatie/ Werkgever	Het roosterproces zorgt voor een sluitende operationele planning voor de organisaties waarbij voldoende en gekwalificeerde medewerkers op het juiste moment aanwezig zijn. Tegelijkertijd zorgt de RRA voor een uniforme toepassing van CAO en ATW. Dat wil zeggen dat: • De juiste toelagen en vergoedingen door de RRA worden toegekend op basis van gelopen roosters. • Bij het roosteren automatische controle plaatsvinden op (voldoende)rusttijden en (maximale)arbeidstijden.

Gebruikersorganisatie/ Medewerker	• Mogelijkheid om werk- en privé zoveel mogelijk op elkaar af te stemmen, dmv: ○ Meeroosteren ○ Ruilmogelijkheden ○ Indienen van roosterwensen • De juiste toelagen en vergoedingen worden door de RRA toegekend op basis van gelopen roosters. • Bij het roosteren automatische controle plaatsvinden op (voldoende) rusttijden en(maximale) arbeidstijden.
O&P Rijk	O&P Rijk biedt roosterdienstverlening aan en voorziet in de correcte verloning van medewerkers.
ODC Noord / SSC-ICT	Is verantwoordelijk voor de benodigde applicatieservers en databases. Dit beheer zorgt ervoor dat persoonsgegevens binnen het Rijk worden opgeslagen en verwerkt. O&P Rijk is de opdrachtgever van ODC Noord.

7 Verwerkingslocaties

De genoemde gegevensverwerking vindt plaats in Nederland.

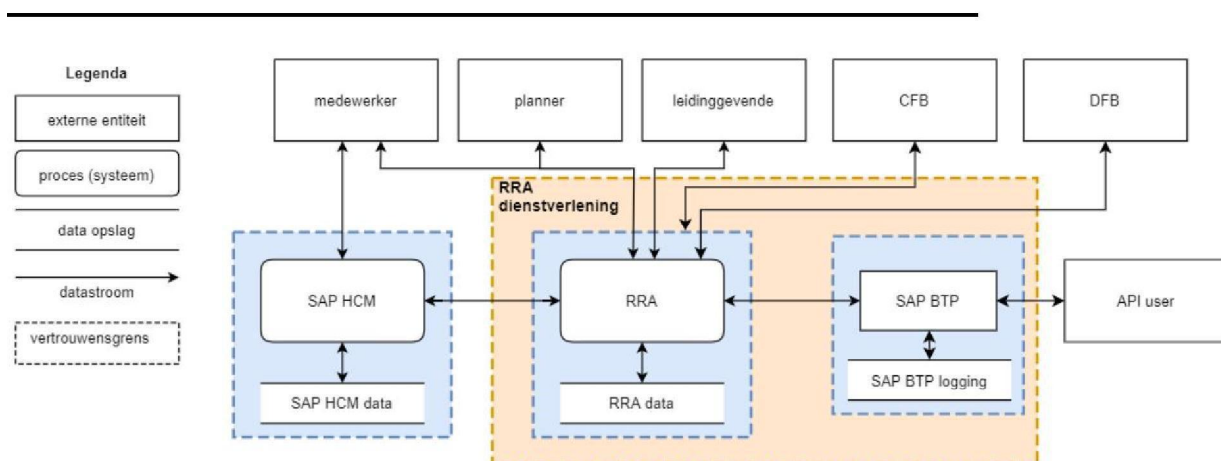
De infrastructuur van de RRA staat in het ODC Noord Rijks Datacenter. De medewerkers, planners en managers (eindgebruikers, inclusief de beheerders) benaderen de RRA via het rijksweb. Dat is een rijksintern netwerk dat voldoet aan de normen toepasselijk voor Departementale Vertrouwelijke informatie. Ook kunnen eindgebruikers een app installeren op een smartphone en/of tablet. De afnemer bepaalt welke toegangsmiddelen worden gebruikt en op welke locaties die is toegestaan.

8 Technieken en methoden van de gegevensverwerkingen

De RRA is een rooster applicatie die bestaat uit verschillende modules. De kern van de RRA bestaat uit de Inplanning 'Planning' module. In aanvulling hierop kan gebruik gemaakt worden van aanvullende modules, zoals 'Vakantieplanning', 'Takenplanning', 'Capaciteitplanning', 'Flexpoolplanning', etc. De RRA kent een koppeling met SAP HCM (HR-systeem) van O&P Rijk. Deze sectie beschrijft de technische inrichting van de RRA-oplossing waarin persoonsgegevens worden verwerkt.

De RRA is te gebruiken via web-browsers. Hiernaast hebben gebruikers de mogelijkheid om de RRA te gebruiken middels een mobiele app, welke is ontwikkeld door Intus. Intus is de leverancier van Inplanning en heeft ook deze app ontwikkeld. Intus verwerkt geen persoonsgegevens (zie hfst. 5).

Afhankelijk van de gekozen roostermethodiek worden de gegevens door de verschillende eindgebruikers verzameld om het roosterproces te ondersteunen. Randvoorwaarden ontstaan door de ingevulde voorkeuren van de medewerkers, uit het toepassen van bedrijfsregels en controles uit voorschriften die komen uit de ATW, en de CAO. Hierdoor is deels sprake van geautomatiseerde (ATW,ATB regels) besluitvorming (zie hfst. 9).



Datastromen in de RRA-oplossing

De RRA is een rooster applicatie met een duidelijke hoofdmodule (Planningsmodule) en optionele aanvullende modules waar het de verwerking van persoonsgegevens betreft. Voor de leesbaarheid van het diagram zijn niet alle softwarecomponenten opgenomen die betrekking hebben op de RRA, maar alleen deze die de processen van persoonsgegevensverwerkingen ondersteunen.

- **Inplanning Planningsmodule** – De kern van de RRA is de Inplanning planningsmodule. SAP HCM is de gegevensbron voor het roosterproces aangevuld met in de RRA toegevoegde informatie (zie hiervoor hfst.2&3). De functionaliteiten zijn gericht op het maken van een rooster en het voeren van een operationele planning om te zorgen voor een adequate bezetting.
- **Inplanning aanvullende modules** –
 - Vakantieplanning: Deze optionele module kan worden gebruikt voor het maken van een vakantieplanning met oog op (voldoende) bezetting.
 - Takenplanning: Deze optionele module kan worden gebruikt voor het voeren van een verfijnde planning waarbij taken worden toebedeeld aan diensten.
 - Opdrachtenplanning: Deze optionele module kan worden gebruikt voor het voeren van een verfijnde planning waarbij opdrachten worden toebedeeld aan diensten.

- Flexpoolplanning: Deze optionele module kan worden gebruikt voor het samenstellen en alloceren van een flexibele schil van medewerkers.
- Capaciteitsplanning: Deze optionele module kan worden gebruikt voor het anticiperen op benodigde- en beschikbare personeelscapaciteit.
- **RRA Ruleset** – De RRA ruleset evalueert de ingeplande werktijden in de RRA en gebruikt dit om:
 - De gebruiker te informeren(in de vorm van meldingen) over eventuele ATW/CAO overschrijdingen;
 - Gebruiker te informeren (in de vorm van meldingen) over (on)juist gebruik van het systeem;
 - Vaststellen van de juiste vergoedingen en toelagen;
 - Bijhouden van verlofsaldo's;
 - Klaarzetten van gegevens t.b.v. uitwisseling met HR.
 Om deze functionaliteit te realiseren is er een directe koppeling tussen de Inplanning applicatie en de RRA ruleset.

De RRA kent koppelingen met externe systemen. Deze systemen worden hieronder genoemd:

- **SAP HCM (Human Capital Management)**– De RRA wisselt persoonsgegevens uit met SAP HCM van O&P RIJK. (zie hiervoor hfst.2&3).
- **SAP BTP (Business Technology Platform)** – SAP BTP bevat de SAP Integration suite, welke beschikt over een API Management tool. De RRA wisselt gegevens uit via SAP BTP middels een API(application programming interface). Via deze route kunnen gebruikersorganisaties informatie onttrekken(secure) uit de RRA, voor zover zij beschikken over autorisatie hiervoor.

Op het niveau van het datastroommodel zijn er de onderstaande categorieën gebruikersgroepen te onderscheiden. Binnen de gebruikersgroepen wordt verder onderscheid gemaakt tussen verschillende rollen, vormgegeven door middel van autorisatie beheer.

- **Gebruikers** – Dit zijn medewerkers/gebruikers van een roosterende gebruikersorganisatie met een rol binnen het roosterproces. Zij hebben toegang tot de RRA en voor zover hun autorisatie toestaat toegang tot persoonsgegevens zoals benodigd voor de goede uitvoering van hun functie. We kennen de volgende type gebruikers van de RRA:
 - **Medewerkers**, dit zijn medewerkers van een roosterende gebruikersorganisatie die geroosterd worden;
 - **Planners**, dit zijn medewerkers van een roosterende gebruikersorganisatie die zich ontfemen over het roosteren;

- **Leidinggevende**, dit zijn medewerkers van een roosterende gebruikersorganisatie met een leidinggevende rol en taken binnen het roosterproces, zoals het beoordelen van verlofaanvragen of het accorderen van urenregistratie;
- **Decentraal functioneel beheerders (DFB)**, dit zijn medewerkers van een roosterende gebruikersorganisatie die de inrichting van de betreffende organisatie beheren. DFB'ers hebben toegang tot de RRA zonder een rol in de kernprocessen. Deze gebruikersgroep voert decentraal functioneel beheer uit op de RRA en ondersteunt medewerkers en gebruikers;
- **Centraal functioneel beheerders (CFB)**, dit zijn medewerkers van een O&P Rijk. CFB'ers hebben toegang tot de RRA zonder een rol in de kernprocessen. Deze gebruikersgroep voert centraal functioneel beheer uit op de RRA en ondersteunt gebruikers;
- **Overige**, Op verzoek van roosterende gebruikersorganisaties kunnen extra rollen worden aangemaakt(door CFB), met een specifieke samenstelling van rechten. Denk aan een Coördinator planner, of bijvoorbeeld een Werkvoorbereider met alleen kijkrechten.

De RRA behandelt alle (persoons)gegevens op het niveau van BBN2. De behandeling van persoonsgegevens is binnen de RRA aan strikte processen gebonden. Alle processen, mensen, hardware en software die worden gebruikt om persoonsgegevens te behandelen zijn gebonden aan Europese richtlijnen voor het beschermen van data. Met de strikte processen en de richtlijnen van de EU draagt de oplossing zorg voor de juiste behandeling van de in de RRA.

Techniek en methode van gegevensverwerking	Ja	Nee	Opmerking
Er is sprake van (semi-)geautomatiseerde besluitvorming	X		Op basis van de gerealiseerde rooster stelt de ruleset automatisch de juiste toelagen en vergoedingen vast op basis van CAO- en ATW regels.
Er is sprake van profilering		X	
Er is sprake van Big Data verwerkingen		X	
Er wordt gebruik gemaakt van encryptie	X		Encryption in transit

Er wordt gebruik gemaakt van pseudonimisering	X	In de OTAP straat wordt gebruik gemaakt van pseudonimisering daarbij worden zo min mogelijk persoonsgegevens meegenomen. Voor een beperkte groep (CFB) is het mogelijk om gegevens te herleiden.
---	----------	--

Met het gebruik van de RRA worden persoonsgegevens van in te roosteren medewerkers centraal opgeslagen. De opslag van de gegevens voldoet aan de Baseline Informatiebeveiliging Overheid (BIO).

Relevante componenten in de RRA maken gebruik van logging waarin geen beveiligingskritieke informatie is opgenomen, wel persoonsgegevens.

Onderstaande tabel biedt een weergave van de technieken benoemd in de AVG:

9 Juridisch en beleidsmatig kader

Wetten

- ATW (Arbeidstijden Wet). Vanuit de ATW en in enkele gevallen de ATB(Arbeidstijdenbesluit) zijn kaders van toepassing op:
 - De werktijden, met betrekking tot minimale rusttijden en maximale arbeidstijden

Beleidsmatig kader

- CAO Rijk. Vanuit de CAO RIJK zijn kaders van toepassing op:
 - De werktijden, met betrekking tot minimale rusttijden en maximale arbeidstijden
 - Verlofrechten
 - Recht op vergoedingen en toelagen

Naast de bovengenoemde, zijn de Archiefwet, de [UAVG](#), de [EU-richtlijn rond arbeidstijden](#) met in het verlengde daarvan de jurisprudentie zoals [minimale dagelijkse rusttijd](#)

10 Bewaartermijnen

Categorie persoonsgegevens	Ingang bewaar-termijn	Termijn van bewaring	Motivatatie bewaring	Verantwoord elijk voor verwijdering
Identificerende persoonsgegevens - Personeelsnummer - RIN Rijks Identifierend Nummer - Naam (Voorletters, Voorvoegsel, Tussenvoegsels, Achternaam, ed.)	Vanaf het moment dat de medewerker voor het laatst is ingeroosterd.	2 jaar	2 jaar ivm in HR gehanteerde toegestane periode voor Payroll mutaties met terug werkende kracht.	O&P RIJK
Adresgegevens - Adres, postcode woonplaats, land	Vanaf het moment dat de medewerker voor het laatst is ingeroosterd.	2 jaar	2 jaar ivm in HR gehanteerde toegestane periode voor Payroll mutaties met terug werkende kracht.	O&P RIJK
Rechtspositionele gegevens - Pers/mdw-subgebied - Schaal - Geboortedatum - Wel/geen recht op vergoeding en toelagen (OVW,TOD/WTV/B&B), - Verlofrechten/saldo's - En dergelijke	Vanaf het moment dat de medewerker voor het laatst is ingeroosterd.	2 jaar	2 jaar ivm in HR gehanteerde toegestane periode voor Payroll mutaties met terug werkende kracht.	O&P RIJK
Geslachtgegevens - Geslacht	Vanaf het moment dat de medewerker voor het laatst is ingeroosterd.	2 jaar	2 jaar ivm in HR gehanteerde toegestane periode voor Payroll mutaties met terug werkende kracht.	O&P RIJK
Werk gerelateerde gegevens - Inzet start- en einddatum - Functie, afdeling - Werktijd/arbeidsduur - Te realiseren uren - 1e en laatste dag arbeidsongeschikt - En dergelijke	Vanaf het moment dat de medewerker voor het laatst is ingeroosterd.	2 jaar	2 jaar ivm in HR gehanteerde toegestane periode voor Payroll mutaties met terug werkende kracht.	O&P RIJK
Roostergegevens - Meeroosteren ja/nee - 'Geen bezwaar tegen nachtdiensten' - Kwalificaties/eigenschappen - Diensttijden - Aan- en afwezigheden - Ziek- en hersteld registratie - Gepland als(functie) - Gepland op(plangroep) - En dergelijke	Vanaf het moment dat de medewerker voor het laatst is ingeroosterd.	2 jaar	2 jaar ivm in HR gehanteerde toegestane periode voor Payroll mutaties met terug werkende kracht.	O&P RIJK
Toegangsgegevens - Username, wachtwoord - autorisatie	Vanaf het moment dat de gebruiker voor het laatst rechten dient te hebben in het systeem.	1 week	De gebruikers / autorisatie worden verwijderd wanneer deze niet meer nodig zijn	O&P RIJK / Gebruikers (rooster) organisatie

B. Beoordeling rechtmatigheid gegevensverwerkingen

11 Rechtsgrond

Gegevensverwerking	Rechtsgrond	Toelichting op de rechtsgrond
Roosteren	Gerechtvaardigd belang	De verwerking is getoetst aan de volgende criteria: 1. De verwerking is een gerechtvaardigd belang. Het is rechtmatig (d.w.z. in overeenstemming met EU en nationaal recht), voldoende duidelijk verwoord (specifiek) en werkelijk aanwezig (niet speculatief). Zonder de betreffende verwerking zou het doeleinde van de verwerking niet mogelijk zijn. 2. De verwerking is noodzakelijk. De inbreuk voor de betrokkene is in verhouding met het doel van de gegevensverwerking (proportionaliteit). Ook is het doel niet op een andere manier te bereiken (subsidiariteit). De verwerking is noodzakelijk voor het verwerkingsdoel. Ook zijn er geen betere alternatieven dan het verwerken van gebruiksgegevens. 3. De belangen van de verwerkingsverantwoordelijke enerzijds en de belangen van de betrokkene anderzijds zijn afgewogen. Het belang van de verantwoordelijke weegt op tegen de inbreuk voor de betrokkene. <i>De volledige uitwerking in terug te vinden in bijlage "Bijlage 1-DPIA RRA- Grondslag gerechtvaardigd belang"</i>

12 Bijzondere persoonsgegevens

Er is geen sprake van verwerking van bijzondere persoonsgegevens.

13 Doelbinding

Er vinden geen verdere verwerkingen van de persoonsgegevens plaats.

De gegevens worden gebruikt om het roosterproces te ondersteunen, inclusief rapportages en statistische onderzoeken en waar nodig gekoppelde systemen te voeden met gegevens. Wanneer van toepassing zijn hiervoor de verwerkingsprocessen en de koppelvlakken beschreven. Deze hangen af van de aansluitende onderdelen van het rijk. Indien gegevens uit het roostersysteem worden geëxporteerd voor een ander doel dan valt de verwerking van die gegevens binnen de verantwoordelijkheid van de desbetreffende organisatie/departement en buiten de scope van deze DPIA programma DOOR.

14 Noodzaak en evenredigheid

De gegevens die worden gebruikt ter ondersteuning van de roosterprocessen vormt de minimaal noodzakelijke set aan gegevens. De genoemde gegevens zijn nodig om te kunnen roosteren en te zorgen voor een correcte uitbetaling van toeslagen en registratie van afwezigheden.

De gegevens die gebruikt worden, zijn nodig om de beschreven taken die behoren bij de beschreven rollen uit te kunnen voeren. Daarbij worden slechts persoonsgegevens gebruikt die in de categorie "gewoon" vallen. De inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen zijn vanuit dat oogpunt evenredig tot de verwerkingsdoeleinden.

Het doel van de RRA is het ondersteunen van het roosteren van medewerkers t.b.v. hun arbeidsovereenkomst én het verlonen conform CAO. Om deze redenen is het noodzakelijk dat persoonsgegevens gebruikt worden. Planners (roosterorganisaties) moeten weten wie ze kunnen inroosteren en medewerkers moeten weten wanneer zij ingeroosterd zijn en dus moeten werken. Voor de juiste toepassing van de CAO en daarmee ook de verloning is het ook noodzakelijk om te weten wie het betreft. Het gebruik van persoonsgegevens is tot het minimum beperkt om te kunnen voldoen aan de doelen van de RRA.

Verder is ervoor gezorgd dat de eindgebruikers slechts toegang krijgen tot de deelverzameling van de gegevens waar zij verantwoordelijk voor zijn, zodat er aan het subsidiariteitsbeginsel voldaan wordt.

Een uitgebreide toets is beschikbaar in *Bijlage 2-DPIA RRA- Proportionaliteit en subsidiariteit*

15 Rechten van betrokkenen

Rechten van betrokkene	Procedure ter uitvoering	Beperking op grond van wettelijke uitzondering
Recht van inzage	Beheerder kan het rapport "RRA_Persoonsgegevens" draaien en de output als PDF met betrokkenen delen.	N.v.t.
Recht op rectificatie en aanvulling	Gegevens kunnen via het P-Direkt Portaal, via de HR-ondersteuner of in enkele gevallen direct in de RRA worden aangepast.	N.v.t
Recht op vergetelheid	Persoonsgegevens kunnen door CFB worden verwijderd uit de RRA. Op dit moment nog wel met inachtneming van de bewaartermijn (2 jaar ivm in HR gehanteerde toegestane periode voor Payroll mutaties met terugwerkende kracht. Hier is in de risico analyse aandacht aan besteed)	N.v.t
Recht op beperking van de verwerking	Verwerking kan zowel in zijn geheel als op onderdelen beperkt worden door CFB.	N.v.t
Recht op dataportabiliteit		N.v.t
Recht niet onderworpen te worden aan geautomatiseerde besluitvorming	Er zijn mogelijkheden om geautomatiseerde besluitvorming achteraf te corrigeren. Doordat: • De planner het rooster aanpast • Er achteraf in het HR systeem aanpassingen of toevoegingen op de looncomponenten doorgevoerd kunnen worden	N.v.t
Recht om bezwaar te maken	Het bezwaar zal door de werkgever gewogen moeten worden. Verwerking kan zowel in zijn geheel als op onderdelen beperkt worden door CFB.	N.v.t
Recht op duidelijke informatie	Uitvoering hiervan is verantwoordelijkheid van werkgever.	N.v.t

O&P Rijk als verwerker ondersteunt de werkgever in de rechten van de betrokkenen zoals in hierboven staande tabel beschreven.

C & D. Beschrijving en beoordeling risico's voor de betrokkenen en maatregelen

16 Risico's voor betrokkenen en 17 maatregelen

Beschrijf en beoordeel de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen.

De risicoanalyse heeft plaatsgevonden in een wisselende, multidisciplinaire samenstelling over meerdere sessies gericht op privacyrisico's in processen, technische inrichting en specifiek de talentenpools. Onderstaande tabel is daarvan het resultaat, met voor elk risico aangegeven in welk onderdeel van het Data Flow Diagram (Hoofdstuk 8) of in welke gegevensverwerking (Hoofdstuk 3) het is risico geïdentificeerd.

Onderstaande risico's zijn niet alle mogelijke privacyrisico's bij de gegevensverwerking ('bruto' risico's), maar de ('netto') risico's zoals geïdentificeerd in de huidige inrichting van de RRA zoals in onderdelen A en B is beschreven. De bestaande situatie is hierin als uitgangspunt genomen.

Voor het inschatten van de ernst van de risico's is de volgende classificatie gebruikt:

kans	omschrijving
1	De kans dat dit zich voordoet in de reguliere verwerking is laag
2	Dit kan met enige regelmaat gebeuren in de reguliere verwerking
3	Zonder maatregelen kan dit frequent gebeuren in de reguliere verwerking
impact	omschrijving
1	De betrokkene ondervindt klein hinder wanneer het risico zich voordoet
2	De betrokkene ervaart concrete, nadelige gevolgen van een privacyschending
3	Het voordoen van het risico heeft zwaarwegende, nadelige gevolgen voor de betrokkene en
ernst	Handelingen
1-2	accepteren, mitigeren of wegnemen
3-5	bij voorkeur mitigeren of wegnemen, anders accepteren
6-9	mitigeren of wegnemen

Per risico is gekeken naar de mogelijke maatregelen. Alternatieve maatregelen zijn waar beschikbaar beschreven. Voor elke maatregel is het type aangegeven (accepteren, mitigeren, wegnemen, opvolgen), waar opvolgen een activiteit betreft buiten de scope van deze DPIA. Bij elke voorgestelde maatregel is een inschatting gemaakt over de nieuwe kans (k), impact (i) en resulterende ernst (e) na toepassing van de maatregel. Een ? bij

ernst betekent dat dit afhankelijk is van keuzes die op het moment van opstellen van deze DPIA nog gemaakt moeten worden.

Bij elk alternatief wordt de maatregel met de minste ernst geadviseerd. Naast de beschreven maatregelen bij de benoemde risico's (die in de matrix hieronder zijn terug te vinden) zijn er een aantal generieke maatregelen getroffen.

Op organisatie niveau zijn de volgende maatregelen getroffen:

Afnemende (rooster) organisaties:

Kunnen gebruik maken van:

- de VOG
- een integriteitsbeleid
- een eed en belofte (verklaring af over functie vervulling als ambtenaar).

<https://www.p-direkt.nl/informatie-rijkspersoneel-2020/rechten-en-regels/integriteit/indiensttreding-en-integriteit/eed-en-belofte>

O&P Rijk:

Verwerker werkt conform de Baseline informatiebeveiliging Overheid (BIO 2018). Risicomanagement in het kader van de BIO is cyclisch en methodisch ingericht op basis van de ISO 27001 en ISO 27002. Voor de (Rijks)overheid vindt nadere specificatie plaats in de algemene voorschriften voor de beveiliging van informatiesystemen: het Beveiligingsvoorschrift Rijksdienst (BVR), het Voorschrift Informatiebeveiliging Rijksdienst (VIR) en het Voorschrift Informatiebeveiliging Rijksdienst - Bijzondere Informatie (VIR-BI).

Verwerker zorgt ervoor dat alle geleverde systemen voldoen aan de richtlijnen of kan verklaren waarom hiervan wordt afgeweken.

Verwerker controleert jaarlijks op technische naleving van de beveiligingsnormen en risico's ten aanzien van de feitelijke veiligheid middels kwetsbaarheidsanalyses of pentesten.

Technische en organisatorische maatregelen

Verwerker specificeert op basis van een risicoanalyse en dataclassificatie adequate technische en organisatorische maatregelen om de risico's ten aanzien van de beveiliging van de (persoons)gegevens, alsmede de rechten en vrijheden van de betrokkenen, die in het kader van deze Opdracht worden verwerkt, af te dekken.

Volgens het veiligheidsbeleid van Organisatie en Personeel Rijk zijn, afhankelijk van de situatie, tenminste de volgende maatregelen genomen:

- Alle medewerkers van de Verwerker:
 - Leggen over de functie vervulling als ambtenaar de Eed of Belofte af.
 - Kunnen bij/vooraf in dienst treden een V.O.G. overleggen.
 - Teken een geheimhoudingsverklaring bij in dienst treding.
- Er is een meldprocedure beveiligingsincidenten, waaronder datalekken, vastgesteld en gecommuniceerd.
- Verwerker geeft structureel uitvoering aan het vastgestelde bewustwordingsplan van Organisatie en Personeel Rijk.

Fysieke maatregelen voor toegangsbeveiliging

Medewerkers krijgen alleen toegang tot de panden en eventuele extra beveiligde ruimtes van de verwerker met de persoonlijke rijkspas.

Bezoekers moeten altijd vooraf aangemeld zijn en begeleid worden binnen de panden.

Rollen en verantwoordelijkheden

De rollen van medewerkers zijn ingericht zodat alleen geautoriseerde medewerkers toegang hebben tot de persoonsgegevens noodzakelijk voor de uitvoering van hun functie. De betreffende toegang/rol wordt verwijderd wanneer deze niet meer noodzakelijk is.

Mobiele apparaten

Alle mobiele apparaten zijn door SSC-ICT beheerd, beveiligd en kunnen op afstand gewist en gelocked worden.

Printen van data is alleen mogelijk op printers een welke zich op kantoor bevindt en niet op een extern (thuis) netwerk.

De verwerker slaat alle data (digitaal en fysiek) altijd beveiligd op.

id	processtap / DFD element	risico	kans	impact	ernst	maatregelen	kans2	impact2	ernst2
1	verkrigen stamgegevens uit SAP HR	Er wordt te veel of foutieve informatie ontvangen bij onjuiste criteria of wisselende status van de medewerker in het bronsysteem	2	2	4	nu: procedure voor handmatige correctie gepland: verbeteren van de synchronisatie tussen systemen	1	2	2
2	verkrigen stamgegevens uit SAP HR	Als iemand uit dienst gaat worden er gegevens aangeleverd zonder doelbinding	1	1	1	zie 1	1	1	1
3	bewaren medewerker stamgegevens	Fouten in autorisaties kunnen leiden tot uitgebreide toegankelijkheid en mogelijke verdere privacyschendingen	1	2	2	Het treffen van maatregelen ligt decentraal bij de afnemers voorgesteld: een jaarlijkse rapportage met overzicht van autorisaties afstemmen met afnemers	1	2	2
4	verkrigen medewerker stamgegevens	Verrijkte informatie kan foutief worden ingevoerd bij een handmatige verwerking (bijv. Meerroosteren, geen bezwaar tegen nachtdiensten)	1	2	2	Het treffen van maatregelen ligt decentraal bij de afnemers	1	2	2
5	verkrigen stamgegevens uit SAP HR	Te veel eigenschappen over een persoon worden toegestuurd vanuit het koppelvak met SAP HR die voor de RRA onwenselijk zijn	1	1	1	Het treffen van maatregelen ligt decentraal bij de afnemers	1	1	1
6	aanmaken/onderhouden RRA gebruikers	O&P Rijk kan fouten maken in het inrichten van de organisatiestructuur waardoor mensen niet zichtbaar zijn in de juiste plangroepen	1	3	3	nu: controle op de invoer tijdens zijn in het proces geborgd gedurende de implementatie en daarna (acceptatie, go live)	1	3	3
7	aanmaken/onderhouden RRA gebruikers	Autorisaties worden niet beëindigd bij een veranderend of beëindigd dienstverband	1	2	2	nu: bij beëindigen dienstverband geen toegang meer tot RRA ivm Rijksaccount Bij functiewijziging wordt dit decentraal beheerd, zie ook 3	1	2	2
8	matchen	Niet alle kenmerken worden in de RRA vastgelegd (bijv. papadagi), wat kan leiden tot conflicterende plannings tussen individu en organisatie	2	2	4	Dit risico is onoverkomelijk in het roosteren, omdat niet altijd alle belangen behartigd kunnen worden. Middels meerroosteren/ruilfunctionaliteit kan een organisatie medewerkers meer inspraak geven.	2	2	4
9	matchen	Een medewerker kan een wens voor het dienstrooster indienen met een (vrije) toelichting, waarvoor de medewerker de noodzaak voelt om te veel informatie te delen	2	2	4	nu: bij de toelichting is aangegeven dat dit optioneel is Het treffen van verdere maatregelen ligt decentraal bij de afnemers	1	2	2
10	matchen	Er kan onderscheid worden gemaakt tussen medewerkers en leiden tot een voorkeursbehandeling bij de inwilliging van (rooster)wensen	1	3	3	gepland: er wordt een overzicht opgesteld met de verdeling van het aantal/type diensten Het treffen van maatregelen ligt decentraal bij de afnemers	1	3	3
11	matchen	Een medewerker kan worden uitgesloten van de verwerking van het matchen, bijv. in het gebruik van eigenschappen en attributen, inwilliging van wensen	1	2	2	nu: een medewerker heeft inzage in hoeverre er aan hun wensen tegemoet is gekomen Het treffen van verdere maatregelen ligt decentraal bij de afnemers	1	2	2
12	bewaren medewerker stamgegevens	Een medewerker ziet niet wat een planner van hen heeft vastgelegd, ze hebben geen inzage in het (volledige) eigen profiel	2	1	2	Beheerder kan het rapport "RRA_Persoonsgegevens" draaien en de output als PDF met betrokkenen delen. Het treffen van eventuele maatregelen ligt decentraal bij de afnemers.	2	1	2
13	roosteren	Verlofaanvragen/ruilverzoeken tijdens het roosteren worden goed- of afgekeurd door de manager, waarbij voorkeursbehandeling plaats kan vinden	1	2	2	Het treffen van eventuele maatregelen ligt decentraal bij de afnemers.	1	2	2
14	roosteren	Een decentraal functioneel beheerder heeft meer rechten dan wenselijk, omdat deze alleen rollen uit kan delen waar deze voor geautoriseerd is. Hiermee heeft deze inzage en wijzigingsrechten op de roosters.	2	1	2	Voorgesteld: in gesprek gaan met de leverancier wat de mogelijkheden zijn om rechten te beperken. De impact hiervan kan nog niet worden vastgesteld. Aangebrachte wijzigingen worden gelogd in het systeem met een user en een wijzigingsdatum. Het treffen van eventuele maatregelen ligt decentraal bij de afnemers.	2	1	2
15	roosteren	Sommige organisaties staan toe dat medewerkers in het groepsrooster kunnen kijken, waarmee ze de aan- en afwezigheid van collega's kunnen bekijken en meer over de persoon kan leren dan wenselijk	2	2	4	Voorgesteld: Afschermen of anonimiseren van data die zichtbaar is voor andere medewerkers	2	2	4
16	matchen	Planner is verantwoordelijk voor ziek- en herstelregistratie in de RRA, waardoor de synchronisatie met SAP HR niet altijd goed gaat en er verschillende administraties ontstaan.	2	2	4	gepland: Wijziging in de manier van registratie van ziekte. SAP HR wordt hierin leidend en de planner gebruikt het alleen voor de planning.	1	2	2
17	matchen	Bij langdurig/gedeeltelijke ongeschiktheid is SAP HR leidend. Aanpassingen in de RRA worden niet doorgevoerd in SAP HR.	2	2	4	gepland: Wijziging in de manier van registratie van ziekte. SAP HR wordt hierin leidend en de planner gebruikt het alleen voor de planning.	1	2	2
18	matchen	Planners zien de verlofsorten en ziek/herstelregistratie ook als ze geen managerrol hebben, wat tot uitgebreide toegankelijkheid leidt	2	1	2	Hierop worden geen maatregelen getroffen, deze gegevens zijn noodzakelijk voor het uitvoeren van de plannersrol.	2	1	2
19	rulesetcontroles op oa CAO/ATW regels	Medewerkers met verkeerde stamgegevens kunnen daar financiële en arbeidsrechtelijke gevolgen van ondervinden tijdens het controleren op de rulesets	1	1	1	Gegevens kunnen via het P-Direkt Portaal, via de HR-ondersteuner of in enkele gevallen direct in de RRA worden aangepast. Er zijn mogelijkheden om geautomatiseerde besluitvorming achteraf te corrigeren. Doordat: •De planner het rooster aanpast •Er achteraf in het HR systeem aanpassingen of toevoegingen op de looncomponenten doorgevoerd kunnen worden	1	1	1
20	matchen	Planners of managers kunnen op individueel niveau afwijken van CAO-bepalingen	1	3	3	Het treffen van eventuele maatregelen ligt decentraal bij de afnemers.	1	3	3
21	rulesetcontroles op oa CAO/ATW regels	Fouten in de werking van de ruleset kunnen worden overgenomen zonder afdoende kritische blik van de eindverantwoordelijke in de daadwerkelijke planning en verloning	1	3	3	Maatregel ingericht door uitgebreid te testen Gepland: - Wijziging in de manier van registratie van ziekte. SAP HR wordt hierin leidend en de planner gebruikt het alleen voor de planning. - Evalueren van verlofintegratie RRA-HR	1	3	3
22	verlof- en verzuim informatie uitwisselen	Er kunnen verschillen ontstaan tussen de verlof- en verzuimadministraties met gevolgen voor de integriteit van de registraties in RRA en SAP HR	2	2	4		1	2	2
23	Toelagen/vergoedingen vaststellen	Planner heeft inzage in uren/percentages voor toelagen en vergoedingen, waardoor deze hierop kan sturen bij het plannen van diensten (voorkeursbehandeling of chantage)	1	2	2	Het treffen van eventuele maatregelen ligt decentraal bij de afnemers.	1	2	2
24	Archiveren/vernietigen roostergegevens	De bewaartermijnen van de gegevens zijn onvoldoende geborgd, waardoor het risico bestaat op verdere privacyschendingen zoals secundair gebruik	2	3	6	Voorstel: Vernietiging inregelen met de juiste bewaartermijnen	1	3	3
25	Archiveren/vernietigen roostergegevens	Het niet tijdig archiveren of schonen van persoonsgegevens (rooster) kan leiden tot meer inzicht in de persoonlijke levenssfeer dan noodzakelijk	2	3	6	Voorstel: Archiveren inregelen met de juiste bewaartermijnen	1	3	3
26	Archiveren/vernietigen roostergegevens	Niet gearchevierde of verwijderde roosters kunnen worden aangepast, inclusief verloning met terugwerkende kracht	1	3	3	Het treffen van eventuele maatregelen ligt decentraal bij de afnemers.	1	3	3
27	Verwijderen medewerker stamgegevens	Onduidelijkheid over bewaartermijnen kan ervoor zorgen dat gegevens onrechtmatig worden bewaard	2	3	6	Voorstel: Vernietiging inregelen met de juiste bewaartermijnen	1	3	3
28	Verwijderen medewerker stamgegevens	Medewerkersgegevens die onterecht (bijv. een fout) worden gesynchroniseerd worden onrechtmatig in het systeem vastgelegd	1	2	2		1	2	2
29	Verwijderen RRA gebruikers en autorisaties	Het niet tijdig bijwerken van autorisaties kan leiden tot onrechtmatige toegang tot persoonsgegevens	1	2	2	Het treffen van maatregelen ligt decentraal bij de afnemers voorgesteld: een jaarlijkse rapportage met overzicht van autorisaties afstemmen met afnemers	1	2	2
30	Inbreuk in de beveiliging	Bij een inbreuk in de beveiliging kunnen de stam- en roostergegevens bij ongeautoriseerde personen terechtkomen, met verdere privacyschendingen als gevolg	1	2	2	Nu: PEN test	1	2	2
31	Datatek	Wanneer een medewerker hun device (ontgrendeld) kwijtraakt is er de kans op een datatek	1	2	2	Voorstel: Account laten uitloggen na bepaalde tijd	1	2	2
32	Planner	Een planner kan uit de roosterdata de locatie en tijd van aan- of afwezigheid afleiden	1	2	2	Het treffen van eventuele maatregelen ligt decentraal bij de afnemers.	1	2	2
33	CFB	Een beheerder kan uit de roosterdata de locatie en tijd van aan- of afwezigheid afleiden	1	2	2		1	2	2
34	CFB/DFB	Een CFber kan een account aanmaken voor een persoon buiten de organisatie of bestaande autorisatiestructuren	1	2	2	Nu: Procedure voor het geven van autorisaties is ingericht Voorgesteld: een jaarlijkse rapportage met overzicht van autorisaties afstemmen met afnemers	1	2	2
35	DFB	Een DFber heeft mogelijk meer inzage in persoonsgegevens dan noodzakelijk omdat het systeem afdwingt dat de toekenners van autorisaties alle rechten heeft van de rollen die deze uit mag delen	1	2	2	Voorgesteld: In gesprek gaan met de leverancier wat de mogelijkheden zijn om rechten te beperken.	1	2	2
36	SAP HCM	De verbinding tussen SAP HCM en RRA is onversleuteld, waardoor de uitgewisselde gegevens voor een derde partij af te luisteren zijn	1	2	2	Nu: PEN test	1	2	2
37	SAP BTP	Als de gegevens van een API worden misbruikt is het niet te achterhalen wie dit was, alleen welke API user de gegevens heeft opgevraagd.	1	2	2	Het treffen van eventuele maatregelen ligt decentraal bij de afnemers.	1	2	2

E. Bijlagen

E1 Toetsen gerechtvaardigd belang

Bijlage 1-DPIA RRA- Grondslag gerechtvaardigd belang

Verwerking: Roosteren

Uitwerking toets:

Wat zijn de voordelen van de verwerking voor de organisatie(s)?

Het roosterproces zorgt voor een sluitende operationele planning voor de organisaties waarbij voldoende en gekwalificeerde medewerkers op het juiste moment aanwezig zijn. Tegelijkertijd zorgt de RRA voor een uniforme toepassing van CAO en ATW. Dat wil zeggen dat:

- De juiste toelagen en vergoedingen door de RRA worden toegekend op basis van gelopen roosters.
- Bij het roosteren automatische controle plaatsvinden op (voldoende)rusttijden en (maximale)werdstijden.

Wat zijn de voordelen voor de betrokkenen?

- Mogelijkheid om werk- en privé zoveel mogelijk op elkaar af te stemmen, dmv:
 - Meeroosteren
 - Ruilmogelijkheden
 - Indienen van roosterwensen
- De juiste toelagen en vergoedingen worden door de RRA toegekend op basis van gelopen roosters.
- Bij het roosteren automatische controle plaatsvinden op (voldoende) rusttijden en(maximale) werdstijden.

Wat zijn de nadelen voor de organisatie(s) als de verwerking niet doorgaat en het doeleinde niet wordt bereikt?

- Bedrijfsvoering kan in het geding komen bij inadequate bezetting
- Verhoogde kans op non compliance met CAO en ATW regels
- Foutieve toekenning van toelagen en vergoedingen

Wat zijn de nadelige gevolgen en risico's voor de betrokkenen?

Dit zijn de risico's zoals beschreven in hfst. 16 van de DPIA.

Welke waarborgen zijn (of worden) getroffen om de risico's en nadelige gevolgen voor de betrokkenen te beperken?

Dit zijn de maatregelen zoals beschreven in hfst. 17 van de DPIA.

Hoeveel persoonsgegevens worden verwerkt?

Er is sprake van een grootschalige verwerking. Op dit moment gaat het om 7000

medewerkers met ca. 30 persoonsgegevens per medewerker, welke zijn beschreven in hfst. 2. van de DPIA.

Wat zijn de redelijke verwachtingen van de betrokkenen?

- Dat er gebruikt gemaakt wordt van juiste en volledige informatie.
- Om te komen tot roosters en het vaststellen van de juiste toelagen en vergoedingen.
- Dat de medewerker tot op zekere hoogte inspraak heeft bij het tot stand komen van de roosters.

Weegt het belang van de verwerkingsverantwoordelijke op tegen de inbreuk op de rechten en vrijheden van de betrokkenen?

Ja, er is een gezamenlijk(werkgever/werknemer) belang om te komen tot roosters, die zorgdragen voor een adequate personeelsbezetting zodat de operationele bedrijfsvoering gewaarborgd is. Tegelijkertijd geeft het roosterproces, ondersteund door de RRA de medewerker de gelegenheid om werk en privé op elkaar af te stemmen.

Er is zorgvuldig gekeken naar de risico's van de betrokkenen en het treffen van adequate maatregelen.

E2 Toets proportionaliteit en subsidiariteit

Bijlage 2-DPIA RRA- Proportionaliteit en subsidiariteit

Verwerking: Roosteren

De verwerking is getoetst aan de criteria van de European Data Protection Supervisor¹.

Uitwerking toets:

Subsidiariteit

Welke fundamentele rechten en vrijheden worden beperkt door de verwerking?

Er wordt inbreuk gemaakt op het recht op privacy, zoals afgeleid uit artikel 8 uit het Europees verdrag voor de rechten van de mens.

Er kan bij het roosteren onderscheidt worden gemaakt op basis van leeftijd en geslacht, wat raakt aan artikel 14 uit het Europees verdrag voor de rechten van de mens.

¹ EDPS (2017), *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit* en EDPS (2019), *EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*, waarvoor het gezamenlijke proces is uitgewerkt in EDPS (2020), *The EDPS quick-guide to necessity and proportionality*.

Wat is het doel/zijn de doelen van de verwerking van persoonsgegevens?

Dit is beschreven in hfst. 4 van de DPIA.

Waarom is de gekozen verwerking essentieel is om het beschreven doel te bereiken?

Er is gekozen voor deze verwerking om de onderstaande zaken te bereiken:

- Een sluitende operationele planning voor de organisaties waarbij voldoende en gekwalificeerde medewerkers op het juiste moment aanwezig zijn, zodat de operationele bedrijfsvoering gewaarborgd is.
- Mogelijkheid om werk- en privé zoveel mogelijk op elkaar af te stemmen, dmv: Meeroosteren, ruilmogelijkheden, indienen van roosterwensen.
- Een rijksbrede uniforme toepassing van de CAO, zodat de juiste toelagen en vergoedingen worden door de RRA worden toegekend op basis van gelopen roosters.
- Automatische controles bij het roosteren op (voldoende) rusttijden en (maximale) arbeidstijden.

Het behalen van deze zaken vergt een, geavanceerde roosterapplicatie met een Rijksbrede inrichting en de beschreven verwerking.

Welke effectieve waarborgen zijn genomen of gepland om de fundamentele rechten en vrijheden van betrokkenen te beschermen?

- Er is gegevensminimalisatie toegepast bij de applicatie en bij de integratie met HR.
- Er zijn in de RRA verfijnde autorisatie mogelijkheden benut om gebruikers uitsluitend rechten te geven voor gegevens die benodigde zijn voor het uitoefenen van de functie.
- Er zijn gegevens (zoals afwezigheidsinformatie) zoveel mogelijk geanonimiseerd/veralgemeniseerd.
- De levens cyclus van persoonsgegevens is in kaart gebracht.
- Er is een uitgebreide risicoanalyse gedaan(hfst.16 van de DPIA).
- Er zijn maatregelen opgesteld voor de beschreven risico's(hfst.17 van de DPIA).

Welke alternatieve, minder indringende verwerkingen kunnen vergelijkbare resultaten opleveren?

De aanleiding voor de ontwikkeling van de Rijksbrede dienst voor roosteren is het programma HNR. Belangrijk resultaat van dit programma is uniformeren en harmoniseren van roosteren binnen het Rijk. Het programma 'Dienstverlening op ondersteuning Roosterprocessen (DOOR) is opgezet om invulling te geven aan deze ambitie.

De Rijksbrede drijfveren voor het implementeren van een centrale Rijksbrede dienst voor roosteren zijn:

- De werk vraag verandert; Duurzaam inzetbaar blijven;
- Tijd-, plaats- en apparaat onafhankelijk werken;
- Meeroosteren (selfservice);
- Professionaliseren roosteren;
- Uniforme verloning conform CAO Rijk;
- Creëren van een eigentijds uniform roosterproces dat de eigenheid van elke uitvoeringsorganisatie binnen het Rijk ondersteunt;
- Op termijn creëren van schaalvoordeel bij ontwikkeling, beheer en digitale procesondersteuning.

Er is gekozen voor een centrale Rijksbrede roosterapplicatie. Met een ruleset die zorgt voor een uniforme toepassing van de CAO. Decentrale roosteroplossingen zouden dezelfde verwerkingen kennen en een uniforme toepassing van de CAO niet bewerkstellingen. De resultaten van alternatieven zouden geen vergelijkbare resultaten opleveren en daarmee niet volstaan.

Proportionaliteit

Wat zijn de voordelen voor de betrokkenen?

Mogelijkheid om werk- en privé zoveel mogelijk op elkaar af te stemmen, dmv:

- Meeroosteren
- Ruilmogelijkheden
- Indienen van roosterwensen
- De juiste toelagen en vergoedingen worden door de RRA toegekend op basis van gelopen roosters.
- Bij het roosteren automatische controle plaatsvinden op (voldoende) rusttijden en (maximale) arbeidstijden.

Wat zijn de nadelige gevolgen en risico's voor de betrokkenen?

Dit zijn de risico's zoals beschreven in hfst. 16 van de DPIA.

Wat zijn de nadelen voor de organisatie(s) als de verwerking niet doorgaat en het doeleinde niet wordt bereikt?

- Bedrijfsvoering kan in het geding komen bij inadequate bezetting
- Verhoogde kans op non compliance met CAO en ATW regels
- Foutieve toekenning van toelagen en vergoedingen

Hoe efficiënt, effectief en belangrijk is de verwerking in het vervullen van het doel/de doelen?

De RRA is een robuuste roosterapplicatie die zich in de markt heeft bewezen als effectief middel om te roosteren. Het centrale karakter en de Rijksbrede

inrichting maakt het middel efficiënt. De doelen van de verwerking hadden niet bereikt kunnen worden zonder de gekozen roosterapplicatie.

Gaat het om kwetsbare personen?

In enkele gevallen gaat het tot op zekere hoogte om kwetsbare personen. Doordat deze personen (zeer) laag zijn opgeleid en/of de Nederlandse taal niet goed beheersen.

Wat is de impact van de verwerking op de betrokkene en is de inbreuk gebalanceerd?

Er wordt inbreuk gemaakt op het recht op privacy, zoals afgeleid uit artikel 8 uit het Europees verdrag voor de rechten van de mens.

Er kan bij het roosteren onderscheid worden gemaakt op basis van leeftijd en geslacht, wat raakt aan artikel 14 uit het Europees verdrag voor de rechten van de mens.

Er is een gezamenlijk(werkgever/werknemer) belang om te komen tot roosters, die zorgdragen voor een adequate personeelsbezetting zodat de operationele bedrijfsvoering gewaarborgd is. Tegelijkertijd geeft het roosterproces, ondersteund door de RRA de medewerker de gelegenheid om werk en privé op elkaar af te stemmen.

Persoonsgegevens worden alleen daar gebruikt waar deze noodzakelijk zijn voor het uitvoeren van de beschreven verwerkingen.

Er is zorgvuldig gekeken naar de risico's van de betrokkenen en er zijn adequate maatregelen beschreven.



Gegevensbeschermingseffectbeoordeling (DPIA)

EZK / RVO / Schade opnemen

Het Instituut Mijnbouwschade Groningen

Groningen, 02-06-2023

Maatregelen
nemen
Privacybewustwording
PIA
Doelbinding
Noodzaak
Effecten in kaart
Bescherming van
persoonsgegevens
Risico's
minimaliseren
Richtinggevend
Rechtsgrond.
Met open vizier

Vaststelling verwerkersverantwoordelijke: Selecteer/typ datum

Naam: portefeuillehouder AVG, dhr. mr. M. Tj. Bouwes

Advies functionaris voor gegevensbescherming: Selecteer/typ datum

Naam: 5.1.2e

Advies CIO: Selecteer/typ datum

Naam:

Gegevensbeschermingseffectbeoordeling (PIA)

EZK / RVO / Schade opnemen
Het Instituut Mijnbouwschade Groningen

Contact:

Ministerie van Economische Zaken, Rijksdienst voor Ondernemend Nederland (RVO)
Het Instituut Mijnbouwschade Groningen (IMG)

Cascadeplein 10
9726 AD Groningen
Hoogezand

contact@schadedoormijnbouw.nl

Versie: 0.1, 2 juni 2023

Inhoudsopgave

Inleiding.....	5
A. Beschrijving kenmerken gegevensverwerkingen.....	6
1. Voorstel	6
2. Persoonsgegevens	6
3. Gegevensverwerkingen	7
4. Verwerkingsdoeleinden	7
5. Betrokken partijen	7
6. Belangen bij de gegevensverwerking	8
7. Verwerkingslocaties	8
8. Techniek en methode van gegevensverwerking	8
9. Juridisch en beleidsmatig kader	9
10. Bewaartermijnen	9
B. Beoordeling rechtmatigheid gegevensverwerkingen.....	10
11. Rechtsgrond	10
12. Bijzondere persoonsgegevens	10
13. Doelbinding	10
14. Noodzaak en evenredigheid	10
15. Rechten van de betrokkene	11
C. Beschrijving en beoordeling risico's voor de betrokkenen.....	11
16. Risico's	11
D. Beschrijving voorgenomen maatregelen.....	12
17. Maatregelen	12

Inleiding

Herziene versie (D)PIA Atabix 1.3.

In verband met de DPIA planning en de Plan Do Check Act-cyclus van het Instituut staat in Q1 van 2023 staat een herziening van de DPIA Atabix 1.3. op de planning. Op 8 maart 2023 heeft er een gesprek plaatsgevonden met de portefeuillehouder. Uit die gesprekken is gebleken dat de werkwijze nauwelijks is veranderd in vergelijking met het verleden. Daarnaast is aan het privacyteam medegedeeld dat Atabix 1.3. medio dit jaar zal worden uitgefaseerd.

Deze (D)PIA wordt n.a.v. de DPIA Atabix 2.0 geactualiseerd. Daarnaast zullen de risico's die volgen uit de aankomende migratie worden besproken en tevens zullen de maatregelen worden geformuleerd om deze risico's te mitgeren. Voor een vergelijking met de PIA uit 2018 verwijst het privacyteam naar bijlage 2.

A. Beschrijving kenmerken gegevensverwerkingen

Beschrijf op gestructureerde wijze de voorgenomen gegevensverwerkingen, de verwerkingsdoeleinden en de belangen bij de gegevensverwerkingen.

Onder A wordt de eerste stap beschreven van de PIA: een overzicht van de relevante feiten van de voorgenomen gegevensverwerkingen. Als de feiten onduidelijk zijn, werkt dit door in de beoordeling.

1. Voorstel



Beschrijf het voorstel waar de gegevensbeschermingseffectbeoordeling op ziet en context waarbinnen deze plaatsvindt op hoofdlijnen.

Het Instituut Mijnbouwschade Groningen (IMG) heeft voor de ondersteuning van de werkzaamheden een applicatie laten bouwen door Atabix Solutions BV. Deze applicatie maakt gebruik van de clouddiensten van Amazon Web Services (AWS) Europe, gevestigd te Luxemburg.

Met deze DPIA worden de risico's en mitigerende maatregelen in beeld gebracht die samenhangen met het gebruik van een publieke cloudoplossing van een Amerikaanse onderneming waarin persoonsgegevens van Nederlandse burgers worden verwerkt.

De scope van de DPIA betreft de keten vanaf het uploaden van de gegevens naar de Atabix applicatie tot en met de handmatige overzetting naar de backoffice applicatie BAS van RVO.nl

Met deze DPIA worden de risico's en mitigerende maatregelen in beeld gebracht die samenhangen met het gebruik van Atabix en de publieke cloudoplossing van AWS (Amerikaanse partij) waarin persoonsgegevens van Nederlandse burgers worden verwerkt.

Het betreft een herziening op de PIA van 2018 jl.

2. Persoonsgegevens



Som alle categorieën van persoonsgegevens op die worden verwerkt. Geef per categorie van persoonsgegevens tevens aan op wie die betrekking hebben. Deel deze persoonsgegevens in onder de typen: gewoon, bijzonder, strafrechtelijk en wettelijk identificerend.

[Klik hier om infotekst te verbergen](#)

Beschrijf allereerst alle te verwerken categorieën van persoonsgegevens. Onder persoonsgegeven wordt verstaan: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.

Natuurlijke personen wil zeggen mensen. Informatie over overleden personen, rechtspersonen, dieren, zaken en