# Privacy Impact Assessment (PIA)

# UWV

# Wet Tegemoetkomingen Loondomein

## *- samenvatting -*

## Inleiding

Volgens de nieuwe Europese privacy verordening (de Algemene Verordening Gegevensbescherming (AVG)) dient de 'verantwoordelijke' vóór de gegevensverwerking een Privacy Impact Assessment (PIA) uit te voeren, wanneer de kans bestaat dat een soort gegevensverwerking gelet op de aard, de omvang, de context en de doeleinden daarvan een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen. De bedrijfsvoering dient voor 25 mei 2018 in overeenstemming te zijn gebracht met de AVG. Ook vanuit de reeds geldende Wet Bescherming Persoonsgegevens (Wbp) wordt vereist dat bedrijven en overheden die persoonsgegevens verwerken 'passende technische en organisatorische maatregelen' nemen om persoonsgegevens te beveiligen.

UWV is een gegevensverwerkende organisatie die gehouden is aan deze wet en regelgeving rondom beveiliging en privacy en hierop actief acteert. Voor de producten van de Wet Tegemoetkomingen Loondomein zijn de privacyaspecten dan ook vanaf het begin van het project meegenomen in de Project Start Architectuur (PSA). Ook Informatie Beveiliging & Privacy(IB&P)-risico's zijn vanaf het begin onderkend en gemitigeerd.

Omdat UWV de beveiliging en privacy van klanten belangrijk vindt en omdat in interviews met het BIT aanbevolen werd een PIA te doen, heeft de stuurgroep WTL september 2017 besloten na de PSA-fase alsnog een PIA te doen om te onderzoeken in welke mate het project WTL UWV voldoet aan de vereisten volgens de kaders van het Privacy Impact Assessment.

Betrokken projectmanagers hebben vervolgens met IB&P-experts de producten en deelproducten van het project WTL in meer detail getoetst met de PIA-checklist UWV. Deze checklist werkt conform Wbp en houdt reeds rekening met de nieuwe vereisten vanuit de AVG. Met deze checklist zijn privacyrisico's en bijhorende maatregelen nader geadresseerd. Met deze notitie wordt een samenvatting gegeven van de uitkomsten van dit assessment en wordt het vervolgtraject geschetst.

## Hoofduitkomsten PIA

Naar voren is gekomen dat de in de PSA geformuleerde kaders ten aanzien van beveiliging en privacy aansluit op de beginselen uit het PIA en daarmee dus de wet- en regelgeving uit Wbp en de AVG. Het PIA gaat dieper op onderwerpen in dan nu in de PSA van Wtl beschreven.

Het PIA WTL UWV heeft aangetoond dat er ten aanzien van de WTL applicatie (inclusief koppelingen met Belastingdienst) geen fundamentele afwijkingen zijn op de beginselen; doelbinding, gegevensminimalisering, beveiliging, kwaliteit en profilering. Aandachtpunten ten aanzien van de beginselen; beveiliging, rechten van betrokkenen, bewaring en vernietiging zijn in beeld. De bijhorende risico's zijn geformuleerd en beheersmaatregelen en actiehouders zijn benoemd.

Geconstateerde bevindingen van het assessment waarop actie is aanbevolen zijn:

- ten aanzien van het doelgroepverklaringenproces, bezwaar- en beroepsproces en het machtigingsproces bestaat nog geen volledige duidelijkheid hoe de PIA-beginselen zijn gewaarborgd. Voorgestelde actie is om scherpte in de privacy-risico's aan te brengen;
- betrek IB&P-officers meer bij het project t.b.v. verdieping en aanvulling;
- houd in de gaten of, waar afgeweken is van de PSA, mogelijk nieuwe beveiligings- en privacy risico's ontstaan zijn.

Deze bevindingen zijn door de stuurgroep overgenomen en hierop is actie ondernomen (zie 'Vervolgtraject)'.

NB: Gedetailleerde deeluitkomsten zijn opgenomen in bijlage 1.

## Hoofdconclusie

Met behulp van het PIA is de noodzaak van de gegevensverwerking WTL voor UWV geëvalueerd en zijn op een gestructureerde wijze de implicaties van de maatregelen en het informatiesysteem op de gegevensbescherming in kaart gebracht. Hierbij is in het bijzonder aandacht besteed aan de beginselen van gegevensminimalisering en doelbinding, de vereisten van een goede beveiliging en de rechten van de betrokkenen.

Het PIA heeft aangetoond dat de beheersing van de beveiligings- en privacy risico's binnen het project WTL UWV in overeenstemming is met het beveiligings- en privacy beleid van UWV en daarmee conform wet- en regelgeving vanuit de Wbp. Ook is het project WTL UWV zich voldoende bewust van de betreffende beveiliging en privacyrisico's. Wel kan op onderdelen de waarborging en inbedding in processen beter worden vormgegeven.

## Vervolgtraject

Op 11 december 2017 heeft de stuurgroep besloten om onderstaande acties in gang te zetten die gepland zijn of momenteel worden uitgevoerd:

1. de awareness en de beheersing van de beveiliging- en privacy risico's ten aanzien van het DGV proces, bezwaar- en beroepsproces en het machtigingsproces te verbeteren bij met name de procesverantwoordelijken van de informatiesystemen en gegevensverzamelingen;
2. de onderdelen die nog in de initiatie/ontwerpfase verkeren, zoals de DLA applicatie, en het bezwaar en beroepsproces en het machtigingsproces per direct een nadere IB&P-analyse uit te voeren en de PSA hierop te actualiseren;
3. de in het PIA geconstateerde IB&P risico's en bevindingen toe te voegen aan de risicolog van het project WTL en deze te voorzien van actiehouders en maatregelen;
4. in het tweede kwartaal van 2018 een Gegevens Effect Beoordeling uit te voeren.

## Bijlage 1 – specifieke deelresultaten

***Deel I. Basisinformatie - type persoonsgegevens, type verwerking, noodzaak en gegevensminimalisering***

| Vraag | Expert opinion |
|---|---|
| **I.1. Specificatie van de persoonsgegevens** | |
| • Vertrouwelijkheidsklasse 3 - Strikt vertrouwelijk | De gegevens voor VIP-pers en eigen personeel zijn afgeschermd voor Uitkeren, in dat geval zal SMZ Bijzondere zaken de beoordeling voor de doelgroepverklaring overnemen.<br>Voor het afgeven van de Doelgroepverklaring wordt geput uit o.a. Uitkeringsgegevens en de registratie in het Doelgroepregister. Juridische Zaken geeft aan dat de gegevens uit de Doelgroepverklaring wordt geschaald in klasse 3, omdat het gegeven dat iemand in een bepaalde doelgroep valt van groot economisch belang is. Als het gegeven openbaar wordt, kan dat invloed hebben op iemands kansen een baan te vinden of om verzekeringen af te sluiten. |
| • Vertrouwelijkheidsklasse 2 - Vertrouwelijk | De gegevens die worden vastgelegd voor Wtl-berekeningen en worden uitgewisseld met de Belastingdienst vallen in Vertrouwelijkheidsklasse 2 (Vertrouwelijk). Dit is in lijn met de classificatie van de als basis gebruikte loonaangiftegegevens voor de berekening. |
| • Vertrouwelijkheidsklasse 1 - Basisniveau | Projectadministratie. |
| • Vertrouwelijkheidsklasse 0 - Openbaar | Communicatie-uitingen WTL. |
| **I.2. Andere specifieke gegevens** | |
| 2a. Gegevens over financiële of economische situatie van de betrokkene, die kunnen leiden tot stigmatisering of uitsluiting | I2a. Gevoelige informatie waaronder bijzondere persoonsgegevens als genoemd in Wbp Artikel 16 en financieel-economische gegevens in relatie tot personen met de indicatiestelling VIP. |
| I.2b. Gegevens over kwetsbare groepen of personen | I2b. Ja, gevoelige informatie waaronder bijzondere persoonsgegevens als genoemd in Wbp Artikel 16 en financieel-economische gegevens in relatie tot werknemers. |
| I.2c. Gebruikersnamen, wachtwoorden en andere inloggegevens | I2c. N.v.t. |
| I.2d. Uniek identificerende gegevens, zoals biometrische | I2d. N.v.t. |

| Vraag | Expert opinion |
|---|---|
| gegevens<br>I.2e. BSN-nummer of een ander persoonsgebonden nummer | <br>I2e. Ja, BSN. |
| **I.3. Noodzaak.** Licht toe per te verwerken type.<br>I.3a. Zijn deze typen persoonsgegevens beleidsmatig of technisch direct van belang en onontbeerlijk voor het bereiken van de beleidsdoelstelling?<br>I.3b. Wat zou er niet inzichtelijk worden als ervoor wordt gekozen bepaalde gegevens niet te verwerken? | <br>I.3a. Ja, noodzakelijk voor het per werknemer vaststellen van recht, hoogte en duur van de tegemoetkoming.<br>I.3b. Het recht, hoogte en duur van de tegemoetkoming. |
| **I.4. Gegevensminimalisering**<br>I.4a. Bij gevoelige persoonsgegevens, kan hetzelfde beleidseffect of technisch resultaat worden bereikt door (gecombineerd) gebruik van normale persoonsgegevens?<br>I.4b. Idem, door gebruik van geanonimiseerde of gepseudonimiseerde gegevens? | <br>I.4a. Ja, dat kan. Waar mogelijk worden gegevens uit de Polis-administratie gebruikt en de materie systemen van de divisie Uitkeren en de afdeling Bijzondere Zaken.<br>I.4b. Nee, is niet mogelijk. Tegemoetkomingen worden per werknemer vastgesteld. |
| **I.5. Gebruik, verwerking en technologie**<br>I.5a. In welk breder wettelijk, beleidsmatig of technisch kader wordt het voorziene beleid, informatiesysteem of gegevensverzameling ontwikkeld?<br>I.5b. Wat voor soort(en) verwerking(en) van persoonsgegevens gaan hiervan deel uitmaken bij het voorziene traject?<br>I.5c. Wordt hierbij gebruikt gemaakt van (nieuwe) technologie of informatiesystemen? | <br>I.5a. De voorziene processen en informatiesysteem en gegevensverzamelingen worden ontwikkeld ten behoeve van de uitvoering van de WTL.<br>I.5b. Registratie van bijzondere persoonsgegevens als genoemd in Wbp Artikel 16 en financieel-economische gegevens van werknemers.<br>I.5c. Voor het berekenen van de tegemoetkomingen wordt gebruik gemaakt van de nieuw ontwikkelde WTL applicatie. Ten behoeve van de registratie van de DGV wordt gebruik gemaakt van een nieuw ontwikkeld DGV-register, DGV-werkadministratie en machtigingenadministratie. |

*Deel 2 - Doelbinding, koppeling, kwaliteit en profilering*

| Vraag | Expert opinion |
|---|---|
| **II.1. Doelen** | |
| II.1a. Wat zijn de specifieke doelen waarvoor de persoonsgegevens worden verwerkt? | II.1a. Het per werknemer vaststellen van recht, hoogte en duur van de tegemoetkoming, ten behoeve van het juist berekenen en uiteindelijke verstrekken van de tegemoetkoming. |
| **II.2. Scenario toevoeging persoonsgegevens** | |
| II.2a. Betreft dit het gebruik van nieuwe persoonsgegevens voor bestaande doelen? | II.2a. Nee, nieuwe gegevens voor nieuw doel (de uitvoering van de WTL). |
| **II.3. Scenario toevoeging doeleinden** | |
| II.3a. Betreft dit nieuwe of aanvullende doeleinden voor bestaande persoonsgegevens door deze te gebruiken, vergelijken, delen, koppelen of anderszins verder te verwerken? | II.3a. Ja, deels. Hergebruik van bestaande gegevens uit de polis en materiesystemen Uitkeren en Bijzonder Zaken. |
| II.3b. Zo ja, hebben alle personen, instanties en systemen die zijn betrokken bij de verwerking dezelfde doelstelling met de verwerking van de desbetreffende persoonsgegevens of is daarmee spanning mogelijk gelet op hun taak of hun belang? | II.3b. Gegevens worden gedeeld met de BD (berekeningen) en SZW (beleidsinformatie). UWV en BD hebben dezelfde doelstelling (uitvoeren WTL). Met een verbijzondering t.a.v. SZW; hierbij gaat het om het analyseren van en verantwoorden over de gerealiseerde effecten van het gevoerde WTL beleid de daartoe geleverde prestaties en de daarmee gemoeide kosten. |
| II.3c. Gelden dezelfde doelen voor het hele proces? | II.3c. Ja. |
| **II.4. Melding aan GD, JZ, FG of CBP** | |
| II.4a. Indien er persoonsgegevens worden uitgewisseld met andere partijen, is er overleg geweest met UWV Gegevensdiensten (GD)? | II.4a. Ja, GD is integraal onderdeel van de uitvoering van het project. |
| II.4b. Is er overleg geweest met UWV Bureau Juridische Zaken (JZ) over het gebruik van deze persoonsgegevens? | II.4b. Ja, JZ heeft een risico analyse afgerond uitgevoerd. |
| II.4c. Indien nieuwe persoonsgegevens worden gebruikt voor een bestaand doel of als een doel wordt toegevoegd voor bestaande persoonsgegevens, hoe wordt dit gemeld aan de UWV Functionaris voor de Gegevensbescherming (FG)? | II.4c. IB&P-functionarissen zijn inmiddels aangehaakt. |

| Vraag | Expert opinion |
|---|---|
| II.4d. Indien er geen UWV FG is, hoe wordt dit gemeld aan het College Bescherming Persoonsgegevens (CBP)? | II.4d. Niet aan de orde. |
| **II.5. Nadere controles**<br>II.5a. Indien nieuwe persoonsgegevens worden gebruikt voor een bestaand doel of als een doel wordt toegevoegd voor bestaande persoonsgegevens, welke (nadere) controles op een dergelijk gebruik zijn voorzien? | II.5a Niet aan de orde. |
| **II.6. Kwaliteit**<br>II.6a. Welke periodieke en incidentele controles zijn voorzien om de juistheid, nauwkeurigheid en actualiteit van de te verwerken persoonsgegevens na te gaan? | II.6a. Bij de berekening voor de Wtl tegemoetkoming wordt inclusief tijdsdimensies vastgelegd welke brongegevens zijn gebruikt, waarmee juistheid en volledigheid kan worden aangetoond. |
| **II.7. Profilering**<br>II.7a. Zullen de verzamelde of verwerkte persoonsgegevens worden gebruikt om het gedrag, de aanwezigheid of de prestaties van de betrokkenen in kaart te brengen of te beoordelen of te voorspellen? | II.7a. Nee, enkel geanonimiseerde statische informatie over het gebruik van de WTL wordt ten behoeve van effectmetingen aan SZW verstrekt. |
| II.7b. Zijn de betrokkenen daarvan op de hoogte? | II.7b. Niet aan de orde (zie II, 7.a). |
| II.7c. Zijn de gegevens die hiervoor worden gebruikt, afkomstig uit verschillende (eventueel externe) bronnen? | II.7c. Niet aan de orde (zie II, 7.a). |
| II.7d. Zijn deze gegevens oorspronkelijk voor andere doelen verzameld? | II.7d. Niet aan de orde (zie II, 7.a). |
| **II.8. Geautomatiseerde vergelijking**<br>II.8a. Wordt bij deze analyse of beoordeling of voorspelling gebruik gemaakt van vergelijking van persoonsgegevens die technisch is geautomatiseerd, dus niet door mensen zelf wordt uitgevoerd?<br>II.8b. Zo ja, hoe wordt geregeld dat, indien dit geautomatiseerde proces tot een beoordeling of voorspelling over een bepaalde persoon leidt, hierop pas concrete actie wordt ondernomen na tussenkomst van en controle door menselijk personeel? | II 8 a en II 8 b: Niet aan de orde. |

***Deel 3 - Betrokken instanties, systemen en verantwoordelijkheden***

| Vraag | Expert opinion |
|---|---|
| **III.1. Instantie of systemen** | |
| III.1a. Welke interne en externe instantie(s) of systemen zijn betrokken bij de voorziene verwerking in elk van de onder I.5 onderscheiden fasen? | III. 1a. Instanties:<br>SZW, BD en UWV (GD Team Bronnen, GD team DWH, GD team Services, Uitkeren (kantoor Alkmaar), Bijzondere Zaken, K&S en SBK. ) |
| III.1b. Welke verstrekkers zijn er en welke ontvangers? | III. 1b.<br>UWV GD (verstrekt en ontvangt gegevens)<br>BD (verstrekt en ontvangt gegevens)<br>SZW (ontvangt gegevens) |
| III.1c. Welke bestanden of deelbestanden zijn er en welke infrastructuren? | III. 1c.<br>1. WTL applicatie > WTL database (afslag Polis-admin. + gegevens WTL)<br>2. WTL gegevensuitwisselingen met BD<br>> Koppelingen EBMS/WUS (4 stuks)<br>> Klantvragen (administratie K3CR & OVB)<br>> Bezwaren BD (administratie GD (OVB)<br>3. DGV-werkadministratie: > Metadata proces vaststellen DGV)<br>4. Doelgroepverklaringenregister: > Metadata DGV-besluit<br>5. Machtigingen administratie: > Machtigingsformulieren<br>6. WTL-gegevensuitwisseling UWV-Gemeenten<br>> Postbus (fase 1)<br>> Koppeling Suwinet (fase 2)<br>7. WTL gegevensuitwisseling UWV-SZW: > Gegevenslevering beleidsinformatie WTL<br>8. WTL gegevensuitwisseling UWV-werkgever/werknemers<br>> Uitgaande stukken voorlopige berekening via BD<br>> In- en uitgaande poststukken DGV-proces (EA)<br>> Postbus machtigingen WTL (EA)<br>9. DWH WTL > Database beleidsinformatie WTL (afslag WTL database, Polis Resa/Fasa ea) |
| | |

| Vraag | Expert opinion |
|---|---|
| **III.2. Verantwoordelijkheid** | |
| III.2a. Is in ieder stadium duidelijk wie verantwoordelijk is voor de verwerking van de persoonsgegevens? | III.2a.<br>1. WTL applicatie > ja<br>2. WTL gegevensuitwisselingen met BD > ja<br>> Wordt vastgelegd in convenanten<br>> Koppelingen EBMS/WUS (4 stuks)<br>> Klantvragen (admin. K3CR & OVB)<br>> Bezwaren BD (admin. GD (OVB?)<br>3. DGV-werkadministratie > ja<br>4. Doelgroepverklaringenregister > ja<br>5. Machtigingen administratie > ja<br>6. WTL-gegevensuitwisseling UWV-Gemeenten > ja<br>7. WTL gegevensuitwisseling UWV-SZW > ja<br>8. WTL gegevensuitwisseling UWV-werkgever/werknemers > ja<br>9. DWH WTL > ja |
| III.2b. Zo ja, is deze persoon of organisatie daarop voldoende voorbereid en geëquipeerd wat betreft de nodige voorzieningen en maatregelen, waaronder middelen, beleid, taakverdeling, procedures en intern toezicht? | III.2b. Ja, wel kan op onderdelen de waarborging en inbedding in processen en procedures beter worden vormgegeven. |
| **III.3. Toegang** | |
| III.3a. Wie binnen uw organisatie, en binnen elk van de andere in de keten betrokken organisaties, krijgen toegang tot de persoonsgegevens? | III.3a. Beheerders en exploitatiemedewerkers binnen UWV en Belastingdienst. |
| III.3b. Bestaat de kans dat de persoonsgegevens ergens binnen de keten ter beschikking komen van onbevoegden? | III.3b. Ja, indien gegeven worden onderschept tijdens de uitwisseling tussen BD en UWV, echter worden de gegevens via beveiligde verbindingen verstuurd. |
| **III.4. Geheimhoudingsverplichting** | |
| III.4a. Geldt voor een of meer van de betrokken instanties een beperking van de mogelijkheid om persoonsgegevens te verwerken als gevolg van geheimhoudingsverplichtingen in verband met een functie of een wettelijke bepaling? | III.4a. ja VIP-ers kunnen enkel door medewerkers van Bijzonder Zaken afgehandeld worden. |
| III.4b. Zijn alle persoonsgegevens die worden verwerkt onder zo een | III.4b. Ja. |

| Vraag | Expert opinion |
|---|---|
| geheimhoudingsverplichting gemarkeerd als Vertrouwelijkheidsklasse 3? | |
| **III.5. Inzichtelijkheid**<br><br>III.5a. Zijn alle stappen van de verwerking in de zin van typen gegevens en uitwisselingen, in kaart gebracht of te brengen, zodanig dat het voor de betrokkenen inzichtelijk is bij wie, waarom en hoe de persoonsgegevens worden verwerkt? | III.5a. Ja. |
| **III.6. Beleid en procedures**<br><br>III.6a. Zijn er beleid en procedures aanwezig of voorzien voor het creëren en bijhouden van een verzameling van de persoonsgegevens die u wilt gaan gebruiken? | III.6a. Ja, IB&P beleid UWV. Convenanten en beheerdocumentatie dienen nog opgesteld te worden. |
| III.6b. Zo ja, hoe vaak en door wie zal de verwerking worden gecontroleerd? | III.6b. Logging en monitoring IB&P aspecten van de verwerking dient nog ingericht te worden conform 'Richtlijn UWV Logging en Monitoring voor IB&P v4.0' |
| III.6c. Omvat de verzameling een verwerking die 'namens u' wordt uitgevoerd, bijvoorbeeld door een onderaannemer? (Zie ook vraag IV.2 over Bewerker.) | III.6c. N.v.t. |
| **III.7. Overdracht buiten de EU/EER**<br><br>III.7a. Is er sprake van overdracht van persoonsgegevens naar een (overheids)instantie buiten de Europese Unie of Europese Economische Ruimte (EU/EER)? | III.7a. N.v.t. |
| III.7b. Heeft dit land een niveau van gegevensbescherming dat als passend is beoordeeld door een besluit van de Europese Commissie of de Minister van Veiligheid en Justitie? | III.7b. N.v.t. |
| III.7c. Worden daarbij alle of een gedeelte van de persoonsgegevens doorgegeven naar die instantie? | III.7c. N.v.t. |

*Deel 4 - Beveiliging, bewaring en vernietiging*

| Vraag | Expert opinion |
|---|---|
| **IV.1. Beleid voor gegevensbeveiliging** | |
| IV.1a. Is het beleid met betrekking tot de gegevensbeveiliging voor de betreffende persoonsgegevens binnen uw organisatie op orde? | IV. 1a. Ja. |
| IV.1b. Zo ja, welke afdelingen zijn binnen de organisatie verantwoordelijk voor het opstellen, implementeren en handhaven hiervan? | IV. 1b. CISO, CDO, JZ, DIV, Coördinatoren IB&P. |
| IV.1c. Is dit beleid specifiek gericht op gegevensbescherming en gegevensbeveiliging? | IV.1c. Ja. |
| **IV.2. Bewerker** | |
| IV.2a. Indien (een deel van) de verwerking bij een andere partij – namelijk een bewerker - plaatsvindt, hoe draagt u zorg voor de gegevensbeveiliging en het toezicht daarop bij die bewerker? | IV.2a. N.v.t.<br>NB: Belastingdienst is in dezen geen bewerker, maar zelfstandig verantwoordelijk voor hun deel van de gegevensverwerking van de Wtl. |
| **IV.3. Beveiligingsmaatregelen** | |
| IV.3a. Welke technische en organisatorische beveiligingsmaatregelen zijn getroffen ter voorkoming van niet-geautoriseerde of onrechtmatige verwerking of misbruik van gegevens die in een geautomatiseerd format staan (zoals wachtwoordbescherming of versleuteling)? | Voor de bouw van de applicaties en koppelingen voor Wtl wordt de SSD norm gevolgd, en als vervolg daarop ook het Security Sign Off proces gevolgd (de validatie of de norm inderdaad voldoende is gehanteerd). Koppelingen binnen en buiten UWV verlopen via de door UWV generiek gebruikte beveiligde 'Systeemintegratie'. Ook wordt voor de koppeling met de Belastingdienst gebruik gemaakt van de bestaande gemeenschappelijke infrastructuur. Toegang tot eigen gegevens via MijnUWV wordt beveiligd door het gebruik van het DigiD.<br><br>IV.3. Algemene UWV procedures zijn van toepassing:<br>o Implementatieplan_Security_ Sign_Off_1.0<br>o IB&P Richtlijn OTAP v1.0<br>o Richtlijn Encryptie V 1.0 |
| IV.3b. Welke maatregelen zijn getroffen voor gegevens die handmatig zijn opgetekend (zoals sloten op kasten)? | IV.3b. Niet aan de orde. |

| Vraag | Expert opinion |
|---|---|
| IV.3c. Zijn er aanvullende maatregelen getroffen ten opzichte van de baseline om gevoelige persoonsgegevens met de Vertrouwelijkheidsklassen 2 en 3 te beveiligen en de toegang te beperken? | IV.3c. De gegevens voor VIP-pers en eigen personeel zijn via een extra technische beveiliging afgeschermd voor de divisies Uitkeren, in dat geval zal SMZ Bijzondere zaken de beoordeling voor de doelgroepverklaring overnemen. |
| **IV.4. Inbreuken**<br>IV.4a. Welke procedures bestaan er in geval van inbreuken op beveiligingsvoorschriften, en voor het detecteren ervan?<br>IV.4b. Is er een calamiteitenplan om het gevolg van een onvoorziene gebeurtenis waarbij persoonsgegevens worden blootgesteld aan onrechtmatige verwerking of verlies van persoonsgegevens af te handelen? | IV.4a. Valt onder verantwoordelijkheid van CISO (UWV ICT Beleid Virusprotectie, Richtlijn UWV Netwerkontsluiting V0.51 en Richtlijn Encryptie V 1.0)<br>IV.4b.<br>Ja, valt onder verantwoordelijkheid van Bestuurszaken. |
| **IV.5. Bewaartermijnen**<br>IV.5a. Hoe lang worden de persoonsgegevens bewaard?<br>IV.5b. Geldt dezelfde bewaartermijn voor elk van de typen van verzamelde persoonsgegevens?<br>IV.5c. Is het project onderworpen aan enige wettelijke of sectorale eisen met betrekking tot bewaring? | IV.5a. Conform Wettelijke bewaartermijn WBP.<br>IV.5b. Nee, er zijn verschillende bewaartermijnen aan de orde.<br>IV.5c. Wettelijke bewaartermijn WBP. |
| IV.5d. Heeft er afstemming plaatsgevonden met UWV DIV over de bewaartermijnen? | IV.5d. Ja. |
| **IV.6. Gronden voor bewaartermijnen**<br>IV.6a. Op welke beleidsmatige en technische gronden is deze termijn van bewaring vereist? | IV.6a. WBP. |
| **IV.7. Vernietigen**<br>IV.7a. Welke maatregelen zijn voorzien om de persoonsgegevens na afloop van de bewaartermijn te vernietigen?<br>IV.7b. Worden alle persoonsgegevens incl. log-gegevens, vernietigd?<br>IV.7c. Is er controle op de vernietiging en door wie? | IV.7a. Vernietiging conform bewaartermijn.<br>IV.7b. Ja.<br>IV.7c. Ja, door Beheerders Bronnen en DIV. |

### *Deel 5 - Transparantie en rechten van betrokkenen*

| Vraag | Expert opinion |
|---|---|
| **V.1. Transparantie** | |
| V.1a. Is het doel van het verwerken van de gegevens bij de betrokkenen bekend of kan het bekend worden gemaakt? | V.1a. Ja, via UWV.nl. |
| **V.2. Informeren van betrokkenen** | |
| V.2a. Indien u de persoonsgegevens direct van de betrokkenen verkrijgt, hoe stelt u hen van uw identiteit en het doel van de verwerking op de hoogte vóór het moment van verwerking? | V.2a. Bij vraag aanvragen van een Doelgroepverklaring wordt de werknemer geïnformeerd over de regeling. Bij het invoeren van de polis-administratie wordt de werkgever geïnformeerd over het doel van de DGV. |
| V.2b. Indien u de persoonsgegevens via een andere (overheids)organisatie verkrijgt, hoe zullen de betrokkenen van uw identiteit en het doel van de verwerking op de hoogte worden gesteld op het moment van verwerking? | V.2b. DGV van gemeenten worden verwerkt door UWV. Gemeenten hebben de verantwoordelijkheid om werknemers op de hoogte te stellen van het gebruik van de door de werknemers beschikbaar gestelde informatie. |
| **V.3. Rechten van betrokkenen** | |
| V.3a. Indien u toestemming tot verwerking van persoonsgegevens aan de betrokkene vraagt (opt-in), kan de betrokkene deze toestemming dan op een later tijdstip weer intrekken (opt-out)? | V.3a. Niet van toepassing: Wtl en de gegevensverwerking hierbij is deel van een wettelijke taak, waarbij toestemming van betrokkenen wettelijk niet is benodigd. |
| V.3b. Bij een weigering toestemming te geven, of bij een intrekking, wat is dan de implicatie voor de betrokkene? | V.3b. Zie antwoord V3a: niet van toepassing. |
| **V.4. Opvragen informatie door betrokkenen** | |
| V.4a. Via welke procedure hebben betrokkenen de mogelijkheid zich tot de verantwoordelijke te wenden met het verzoek hen mede te delen of hun persoonsgegevens worden verwerkt? | V.4a en V4b: Burgers kunnen een inzageverzoek kunnen indienen bij UWV en zo een beroep doen op hun inzagerecht. Dit kan voor elke gegevensverwerking van UWV, ook voor de Wtl. |
| V.4b. Hoe worden derden, die mogelijk bedenkingen hebben tegen een dergelijke mededeling, in de gelegenheid gesteld hun zienswijze te geven? | |
| **V.5. Verzoeken tot correctie door betrokkenen** | |
| V.5a. Hoe wordt een verzoek van een betrokkene tot verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens in behandeling genomen? | V.5a. Burgers kunnen een correctieverzoek indienen bij UWV en hiermee een beroep doen op hun correctierecht. |