

UWV Beleidskader Privacy

Een toelichting op wat de AVG voor UWV betekent

versie 2021



Inhoudsopgave

1. Inleiding	3
1.1. Aanleiding voor het actualiseren van het beleidskader privacy	3
1.2. Doel van het beleidskader	4
1.3. Positionering van het beleidskader, aanvullend beleid en richtlijnen	4
1.4. Leeswijzer	4
1.5. Opbouw van de hoofdstukken	5
1.6. Documentbeheer	5
2. Algemene begrippen	7
2.1. Wat zijn persoonsgegevens?	7
2.2. Wanneer is sprake van een verwerking?	9
2.3. Verwerkingsverantwoordelijke, verwerker en verwerkersovereenkomst	10
2.4. UWV beleidskader algemene begrippen	13
3. Beginselen die gelden voor alle verwerkingen van persoonsgegevens	15
3.1. De verwerking moet rechtmatig zijn	15
3.2. De verwerking moet behoorlijk en transparant zijn	15
3.3. De verwerking moet voldoen aan het beginsel van doelbinding	16
3.4. Er moet sprake zijn van minimale en proportionele gegevensverwerking	18
3.5. De persoonsgegevens die worden verwerkt moeten correct zijn	19
3.6. De bewaartermijn van de persoonsgegevens moet zo beperkt mogelijk zijn	20
3.7. De persoonsgegevens moeten adequaat zijn beveiligd	21
3.8. Privacybeginselen moeten al bij het ontwerpen en inrichten van processen en systemen een plaats krijgen (<i>security & privacy by design/default</i>)	22
3.9. UWV beleidskader privacybeginselen	22
4. Grondslagen voor de verwerking van persoonsgegevens	24
4.1. Noodzakelijk voor uitvoering van een wettelijke taak van algemeen belang	24
4.2. Noodzakelijk voor de uitvoering van een overeenkomst	25
4.3. Noodzakelijk om te voldoen aan een wettelijke verplichting	26
4.4. Noodzakelijk ter behartiging van een gerechtvaardigd belang	26
4.5. Noodzakelijk ter bescherming van een vitaal belang	27
4.6. Verwerking op basis van toestemming van de betrokkene	28
4.7. UWV beleidskader grondslagen	29
5. Verwerkingen van persoonsgegevens bij UWV	30
5.1. Bijzondere persoonsgegevens	30
5.2. Persoonsgegevens van strafrechtelijke aard	37
5.3. Burgerservicenummer (BSN)	39
5.4. Verwerking van spontaan verstrekte persoonsgegevens	40
5.5. Ontvangen en verzamelen van persoonsgegevens	41
5.6. Delen en verstrekken van persoonsgegevens	41
5.7. Gebruik van open bronnen (Google, social media, openbare registers)	45
5.8. Analyse, profilering en geautomatiseerde besluitvorming	46
6. Bewaren en vernietigen van persoonsgegevens	55
7. Beveiliging van persoonsgegevens	58
7.1. De Baseline Informatiebeveiliging Overheid (BIO)	58
7.2. Toegang tot persoonsgegevens en autorisatiebeheer	59
7.3. Classificeren van gegevens (BIV-classificatie)	61
7.4. Veilig communiceren van persoonsgegevens	62
8. Transparantie en verantwoording	65
8.1. Informatie over de verwerking aan betrokkene (privacyverklaring)	65
8.2. Register van verwerkingen	67
9. Rechten van betrokkenen	68
9.1. Verzoek om inzage in persoonsgegevens	69
9.2. Verzoek om correctie van persoonsgegevens	70
9.3. Verzoek om verwijdering van persoonsgegevens	71

9.4. Verzoek om de verwerking tijdelijk stil te leggen ('beperking')	71
9.5. Recht om bezwaar te maken tegen de verwerking	72
9.6. Uitzonderingen op de rechten van betrokkenen	73
10. Functionaris Gegevensbescherming (FG)	75
11. Instrumentarium en specifieke procedures	77
11.1. Gegevensbeschermingseffectbeoordeling (GEB)	77
11.2. Melden van beveiligingsincidenten en datalekken	78
11.3. Schadeclaim bij datalek	80
11.4. Melding wijzigingen register van verwerkingen	80
Lijst van afkortingen	82
Bijlage I Overzicht relevante beleidsstukken en instructies	83

1. Inleiding

Het recht op privacy is een fundamenteel recht dat in het Europees Verdrag voor de rechten van de mens is vastgelegd. In artikel 8 lid 1 van dit verdrag staat geschreven:

*Een ieder heeft recht op respect voor zijn privé leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.*¹

Onder invloed van de ontwikkeling van computers, netwerken en databases waar grote hoeveelheden persoonlijke gegevens kunnen worden opgeslagen, is de aandacht voor privacy in de afgelopen decennia steeds meer gericht op informatiele privacy en het beschermen daarvan. Hoewel privacy een breder begrip is en bijvoorbeeld ook bescherming van de fysieke persoonlijke sfeer omvat, gaat het in dit beleidskader over de bescherming van persoonsgegevens, dat wil zeggen informatiele privacy.

UWV verwerkt van ruim 13 miljoen burgers persoonsgegevens. Het gaat om gegevens van uitkeringsgerechtigden en werkzoekenden, van personen die in de polisadministratie staan geregistreerd, maar ook om gegevens van medewerkers of relaties van UWV. Het gaat veelal om gevoelige gegevens die direct of indirect iets prijs geven van de persoonlijke aangelegenheden van burgers – en hen daarmee in hun privacy raken.

UWV heeft legitieme redenen om deze gegevens te verwerken. In de eerste plaats voor het uitvoeren van zijn wettelijke taken die voortkomen uit de Wet SUWI, andere sociale zekerheidswetten (materiewetten) en andere wetten. Maar daarnaast ook in de rol van grote werkgever en als organisatie die contracten sluit met derden, bijvoorbeeld in het kader van de bedrijfsvoering. Bij de verwerking van persoonsgegevens heeft UWV de plicht om vertrouwelijk met deze gegevens om te gaan en de privacy van burgers te respecteren en te beschermen.

UWV hecht daarom groot belang aan de zorgvuldige omgang met persoonsgegevens. Onze klanten, medewerkers en contractpartners moeten erop kunnen vertrouwen dat hun persoonsgegevens bij UWV in veilige handen zijn. Dat geldt te meer omdat, waar het onze klanten betreft, zij in de meeste gevallen niet vrij zijn om voor onze dienstverlening te kiezen. Burgers met een arbeidsbeperking of die werkloos zijn geworden, zijn vaak voor een inkomen afhankelijk van de diensten van UWV. En de polisadministratie, die UWV beheert, bevat de verplichte registratie van persoonsgegevens van alle werknemers in Nederland met betrekking tot hun inkomstgegevens zoals arbeidsvergoedingen, sociale uitkeringen, lijfrentes en pensioenen.

Naast de verantwoordelijkheid om zorgvuldig met persoonsgegevens om te gaan, rust op UWV ook de verantwoordelijkheid om de continuïteit van de aan UWV opgedragen dienstverlening te kunnen borgen. Hoewel bescherming van privacy een intrinsiek onderdeel vormt van betrouwbare en goede dienstverlening, kunnen de belangen van het waarborgen van een continue dienstverlening in sommige situaties spanning opleveren met het doorvoeren van privacy-maatregelen. Bij de verdere besluitvorming over de implementatie van dit beleidskader, zullen afwegingen in dit verband aan de orde komen.

1.1. Aanleiding voor het actualiseren van het beleidskader privacy

In december 2018 heeft de Raad van Bestuur de eerste versie van dit UWV Beleidskader Privacy vastgesteld. Toen is ook door de Raad opgemerkt dat het stuk actueel moet blijven en dus na verloop van tijd moet worden geactualiseerd. In 2020 is de eerste actualisatie van het beleidskader opgepakt en in maart in de Raad van Bestuur vastgesteld. Inmiddels is opnieuw een jaar verstreken en is het wederom tijd om het beleidskader op onderdelen bij te werken.

¹ Artikel 8 lid 2 EVRM geeft de voorwaarden waaronder de overheid bevoegd is inbreuk op dit recht te maken. Artikel 8 lid 2 luidt: 'Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.'

Het is daarbij van belang om op te merken dat het beleidskader nog niet op alle onderdelen een weergave is van de huidige situatie, maar een beeld schetst waar UWV aan zou moeten voldoen om met recht te kunnen stellen dat UWV aan de AVG voldoet.

1.2. Doel van het beleidskader

Het doel van dit beleidskader is de voor UWV belangrijkste verplichtingen uit de AVG te vertalen naar de (beoogde) praktijk van UWV. Daarmee wil het voor medewerkers uitleg geven over wat er van UWV op dit terrein wordt verwacht en tracht het onduidelijkheid op bepaalde thema's weg te nemen. Binnen UWV zijn in de loop der tijd op deelterreinen beleidsstukken en instructies verschenen in verband met privacyregelgeving. Dit beleidskader beoogt ook te verduidelijken welke plaats deze stukken in het grotere geheel innemen. Daarnaast heeft het beleidskader tot doel richting de Autoriteit Persoonsgegevens aan te tonen op welke wijze UWV uitvoering geeft aan de AVG.² Hoewel het zwaartepunt van het beleidskader ligt bij de verwerking van persoonsgegevens van klanten van UWV, gelden de principes die hierin zijn omschreven ook voor de verwerking van persoonsgegevens van medewerkers van UWV of van relaties van UWV.

1.3. Positionering van het beleidskader, aanvullend beleid en richtlijnen

Dit UWV-brede beleidskader privacy beoogt het overkoepelende en kaderstellende basisdocument te zijn, waarin richting en uitleg wordt gegeven hoe binnen UWV met privacy wordt omgegaan. Sommige onderwerpen die in dit beleidskader in meer algemene termen worden besproken behoeven een nadere verdieping in aanvullend beleid of richtlijnen. Voorbeelden hiervan zijn de *Handleiding gebruik BSN UWV (JZ)* en de *Instructie Gegevensverstrekking aan Derden (Gegevensdiensten in afstemming met JZ)*. Er bestaat echter ook behoefte aan verdieping op een aantal andere onderwerpen. Het gaat bijvoorbeeld om:

- omgang met persoonsgegevens van medewerkers (HRM);
- analyseomgevingen (Data Office/Gegevensdiensten);
- Data Lifecycle Management (Data Office/Gegevensdiensten);
- omgang met gezondheidsgegevens (SMZ);
- gebruik van (digitale) communicatiemiddelen richting klanten (K&S);
- het gebruik van foto's, videobeelden en andere persoonsgegevens voor communicatiedoeleinden, waaronder social media (Concerncommunicatie);
- het gebruik van cookies en andere tracking tools (K&S)³.

Het aanvullende beleid dat hierover vanuit de organisatieonderdelen nog zal worden opgeleverd, wordt na advies van de Functionaris Gegevensbescherming (FG) door de Raad van Bestuur vastgesteld en geldt dan voor heel UWV. De FG toetst in dit proces onder andere of het voorgestelde aanvullende privacybeleid in lijn is met het UWV beleidskader privacy.

Naast de UWV-breed geldende beleidsstukken en richtlijnen, kan binnen een organisatieonderdeel de behoefte bestaan om een bepaald onderwerp voor dat organisatieonderdeel meer gedetailleerd uit te werken. Dit kan ertoe leiden dat een organisatieonderdeel aanvullende richtlijnen of instructies ontwikkelt die specifiek gelden voor de processen en verwerkingen van persoonsgegevens die binnen dat organisatieonderdeel spelen (en dus niet voor de andere organisatieonderdelen gelden). Indien een organisatieonderdeel inderdaad aanvullende privacyrichtlijnen opstelt, dient de Functionaris Gegevensbescherming (FG) voorafgaand aan vaststelling daarvan te toetsen of de richtlijn in lijn is met het dit algemene privacy beleidskader.

1.4. Leeswijzer

In dit beleidskader wordt een toelichting gegeven op wat de AVG voor UWV betekent. In de eerste drie hoofdstukken wordt de basis van de AVG besproken: de algemene begrippen van de AVG (*artikel 4 AVG*) worden uitgelegd in hoofdstuk 2. Hierin wordt bijvoorbeeld nader gedefinieerd wat persoonsgegevens en verwerkingen zijn en hoe het zit met de verwerkingsverantwoordelijke en verwerker. In hoofdstuk 3 worden de beginselen van de AVG (*artikel 5 AVG*) besproken en in hoofdstuk 4 wordt ingegaan op de grondslagen voor de verwerking van persoonsgegevens (*artikel 6 AVG*). Samen vormen deze hoofdstukken een toelichting op het hart van de AVG; de artikelen die altijd van toepassing zijn bij het verwerken van persoonsgegevens.

² Artikel 24 AVG.

³ Dit beleid ziet niet op het gebruik van cookies of andere tracking tools die mogelijk gebruikt worden op DWU of andere interne systemen van UWV.

In de daarop volgende hoofdstukken wordt ingegaan op een aantal verwerkingen zoals die voorkomen bij UWV en ten aanzien waarvan binnen UWV behoefte bestaat aan verduidelijking. [Hoofdstuk 5](#) bespreekt onder andere de verwerking van extra gevoelige persoonsgegevens, waaronder het BSN, het verstrekken (delen) van persoonsgegevens en de verwerking van persoonsgegevens voor analyses. [Hoofdstuk 6](#) gaat specifiek in op het bewaren en vernietigen van persoonsgegevens.

Na het bespreken van deze verwerkingen, gaat [hoofdstuk 7](#) in op de beveiliging van de persoonsgegevens, waarbij een relatie met de Baseline Informatiebeveiliging Overheid (BIO) wordt gelegd. Ook wordt hier ingegaan op autorisatiebeheer en veilige communicatie van persoonsgegevens.

In hoofdstuk 8 en 9 verschuift het perspectief waarmee naar privacy wordt gekeken naar buiten. In [hoofdstuk 8](#) wordt besproken wat de AVG-verplichting tot transparantie voor UWV betekent, hoe betrokkenen over verwerkingen worden geïnformeerd en hoe UWV zich over deze verwerkingen verantwoordt. In [hoofdstuk 9](#) wordt vervolgens ingegaan op de rechten van betrokkenen en hoe deze worden gewaarborgd.

[Hoofdstuk 10](#) geeft een toelichting op de rol en taken van de Functionaris Gegevensbescherming (FG) en hoe de FG binnen UWV is gepositioneerd. En tot slot wordt in [hoofdstuk 11](#) nog ingegaan op een aantal specifieke AVG-instrumenten en procedures.

In de bijlage wordt een overzicht gegeven van andere stukken, in het bijzonder UWV beleidsstukken, die in dit beleidskader worden genoemd.

1.5. Opbouw van de hoofdstukken

De hoofdstukken in dit beleidskader zijn volgens een vast stramien opgebouwd: eerst wordt in een blauw kader kort aangegeven wat de AVG over het betreffende onderwerp zegt. Dit betreft niet de letterlijke tekst van de AVG, maar een vertaling daarvan in iets toegankelijker taalgebruik. Het blauwe kader wordt gevolgd door een toelichting op het onderwerp, waarbij nader wordt ingegaan op wat dit voor UWV betekent. Uiteindelijk wordt het hoofdstuk (en bij lange paragrafen ook de paragraaf zelf) afgesloten met een grijs dikgedrukt kader waarin de beleidsuitspraken voor UWV met betrekking tot dat onderwerp nog eens kort zijn opgesomd.

1.6. Documentbeheer

Op 11 december 2018 is de eerste versie van dit document (versie 1.0) na een uitgebreide reviewronde door de organisatieonderdelen door de Raad van Bestuur vastgesteld. Het beheer is belegd bij Bureau Gegevensbescherming. Om ervoor te zorgen dat het beleidskader actueel blijft, is in december 2019 een actualiseringslag gemaakt. De geactualiseerde versie (versie 2.0) is eveneens door de Raad van Bestuur vastgesteld.

Versie	Datum	Verskil met voorgaande versie	Distributie
1.0 (versie 2019 def.)	11-12-2018	Eerste versie (2019) vastgesteld door RvB	BSO's en publicatie DWU
1.5	02-01-2020	Aanpassingen van BG en JZ voor geactualiseerde versie 2020	FG
1.8	10-01-2020	Feedback FG verwerkt	CISO en BSO's SMZ, K&S, UIT, GD. Werkbedrijf, FB, DHH en C-ICT
1.9	13-02-2020	Opmerkingen BSO's verwerkt	RvB
2.0 (versie 2020 def.)	03-03-2020	Tweede versie (2020) vastgesteld door RvB	Directeuren, BSO's en publicatie op DWU
2.5	23-02-2021	Aanpassingen gezondheidsgegevens	JZ, CEC
2.6	24-06-2021	Feedback CEC en JZ verwerkt	JZ, CEC, GD en Data Office
2.7	30-06-2021	Aanpassingen van BG voor geactualiseerde versie 2021	JZ, CEC, GD en Data Office
2.8	02-07-2021	Feedback JZ en CEC verwerkt	Tactisch Overleg van de coalitie IB&P
2.9	22-07-2021		Strategisch overleg van de coalitie IB&P

2. Algemene begrippen

Voor een goed begrip van dit beleidskader en de reikwijdte ervan, is het van belang om enkele cruciale begrippen uit de AVG nader toe te lichten. Dit hoofdstuk strekt daartoe.

2.1. Wat zijn persoonsgegevens?

Wat zegt de AVG?

Onder persoonsgegevens wordt verstaan alle informatie met betrekking tot een persoon. Dit kan een persoon zijn waarvan de identiteit al bekend is of een nog onbekende persoon die aan de hand van die gegevens kan worden geïdentificeerd. Het gaat zowel om digitale gegevens als gegevens die op papier staan. De persoon waarop persoonsgegevens betrekking hebben wordt de 'betrokkene' genoemd.

Artikel 4 onder (1) AVG

Bij persoonsgegevens gaat het in de eerste plaats over alle informatie die betrekking heeft op een reeds geïdentificeerde persoon, zoals op een bepaalde klant, een bepaalde medewerker etc. Het gaat hierbij niet alleen om informatie die systematisch is opgeslagen in de doelsystemen⁴, maar bijvoorbeeld ook om aantekeningen van een medewerker over een gesprek met een klant of een e-mail die informatie over een persoon bevat.

Daarnaast gaat het om gegevens aan de hand waarvan een persoon direct of indirect kan worden geïdentificeerd. Met indirect wordt bedoeld dat een combinatie van gegevens kan leiden tot de identificatie van een bepaalde persoon. Voorbeelden hiervan zijn een naam, adres, woonplaats, geboortedatum, geboorteplaats, een identificatienummer (zoals het BSN). Maar ook bepaalde online-identificatoren (zoals locatiegegevens, een IP-adres of een tracking-cookie) kunnen persoonsgegevens bevatten.

Kort gezegd: alle informatie die op een of andere manier aan een individu is te verbinden of kan worden verbonden, valt onder het begrip persoonsgegevens.

Ook persoonsgegevens die openbaar zijn, bijvoorbeeld omdat ze zijn opgenomen in een openbaar register zoals het Kadaster of de Kamer van Koophandel of door de betrokkene zelf zijn geopenbaard op een website of via social media, vallen onder de regels van de AVG. Dit betekent dat wanneer UWV openbare persoonsgegevens wil verzamelen en gebruiken, dit ook aan de eisen van de AVG moet voldoen (zie ook paragraaf 5.7)

Uit de definitie van persoonsgegevens volgt dat veruit de meeste gegevens die UWV verwerkt, persoonsgegevens zijn. De belangrijkste categorieën van personen van wie UWV persoonsgegevens verwerkt zijn:

- klanten van UWV (uitkeringsgerechtigden, werkzoekenden, vrijwillige verzekerden, personen over wie een sociaal-medisch oordeel wordt gevraagd);
- personen die in de polisadministratie zijn opgenomen;
- bezoekers van UWV (zowel van de gebouwen als 'digitale' bezoekers van de portalen en websites);
- contactpersonen van werkgevers en re-integratiebureaus;
- personen die aan UWV goederen of diensten leveren;
- medewerkers van UWV⁵;
- uitzendkrachten, externe adviseurs en andere personen die UWV inhuurt.

⁴ In dit beleidskader wordt regelmatig de term doelsystemen gebruikt. Hiermee wordt bedoeld op systemen, ook wel procesapplicaties genoemd, die specifiek zijn aangewezen voor de ondersteuning bij de uitvoering van een (deel)proces van de wettelijke taken van UWV. Denk bijvoorbeeld aan applicaties als WWO en Sonar.

⁵ HRM is verantwoordelijk voor het privacybeleid ten aanzien van personeelsgegevens.

2.1.1. Extra gevoelige persoonsgegevens

De AVG en UAVG kennen drie categorieën van persoonsgegevens die extra gevoelig van aard zijn en daarom extra worden beschermd. Dit betekent niet dat deze gegevens per definitie niet door UWV mogen worden verwerkt, maar dat aan de verwerking strengere regels zijn verbonden dan aan de verwerking van 'gewone' persoonsgegevens. Wanneer UWV dergelijke gegevens wil verwerken, is dus extra alertheid geboden. Het gaat om de volgende drie categorieën persoonsgegevens:

- bijzondere persoonsgegevens (artikel 9 AVG) (zie verder paragraaf 5.1)
- persoonsgegevens van strafrechtelijke aard (artikel 10 AVG) (zie verder paragraaf 5.2)
- burgerservicenummer (BSN) (artikel 87 AVG en 46 UAVG) (zie verder paragraaf 5.3)

In hoofdstuk 5 wordt ingegaan op de vraag welke van deze gegevens UWV mag verwerken en onder welke voorwaarden.

2.1.2. Geanonimiseerde (persoons)gegevens

Wanneer persoonsgegevens onomkeerbaar zijn geanonimiseerd en ook niet op een andere wijze, bijvoorbeeld door het combineren van bepaalde gegevens, zijn te herleiden tot een bepaalde persoon, is er niet langer een risico voor de privacy van de betrokkene – zijn of haar identiteit is immers niet langer bekend. Onomkeerbaar geanonimiseerde gegevens zijn daarom geen persoonsgegevens in de zin van de AVG en de verwerking van dergelijke gegevens hoeft dan ook niet meer te voldoen aan de AVG.

Voor de volledigheid wordt opgemerkt dat de eisen waaraan moet worden voldaan wil men met recht kunnen spreken van geanonimiseerde of anonieme (persoons)gegevens strikt zijn. Vanwege het feit dat UWV over een zeer grote hoeveelheid gegevens van klanten beschikt, zal zeer nauwkeurig moeten worden gekeken of de bewerking van de gegevens inderdaad zodanig is dat de identiteit van betrokkenen niet meer (direct of indirect) is te herleiden. Als hierover twijfel bestaat verdient het de voorkeur om ervan uit te gaan dat de gegevens niet volledig en onomkeerbaar zijn geanonimiseerd. Dat betekent dat de verwerking vervolgens aan de eisen van de (U)AVG en dit beleidskader moet voldoen.

Ook bij het verzamelen van gegevens over het online-gedrag van gebruikers van de website van UWV moet zorgvuldig worden gekeken of al dan niet sprake is van anonieme persoonsgegevens. Zo is het IP-adres of de data van een (tracking-)cookie in de meeste gevallen een persoonsgegeven en zal het vastleggen daarvan dus aan de eisen van de (U)AVG en dit beleidskader moeten voldoen.

UWV stelt verschillende rapportages op waarin gegevens op geaggregeerd niveau worden weergegeven. Dat betekent dat uit die rapportage geen informatie over individuen is te herleiden.⁶ Hierdoor bestaat geregeld het misverstand dat het opstellen van dergelijke rapportages geen verwerking in de zin van de AVG zou zijn. Dat is in veel gevallen een onjuiste veronderstelling omdat voor het opstellen van die rapportage vaak eerst analyses zijn verricht met behulp van tot individuen herleidbare persoonsgegevens (op BSN-niveau). Dit betekent dat ook dergelijke analyses die bedoeld zijn om uiteindelijk een rapportage op geaggregeerd niveau op te stellen, eveneens aan de regels van de (U)AVG en dit beleidskader moeten voldoen. (zie ook paragraaf 5.8)

2.1.3. Gepseudonimiseerde persoonsgegevens

Een goede methode om persoonsgegevens af te schermen of te beveiligen tegen onnodige of onbevoegde kennisneming, is de persoonsgegevens te pseudonimiseren. Pseudonimiseren is een techniek waarbij persoonsgegevens volgens een bepaald algoritme worden versleuteld, zodat zij niet als zodanig zichtbaar zijn. Wel kunnen ze, door het algoritme te gebruiken, weer worden ontsleuteld en als zodanig zichtbaar worden gemaakt. In dit opzicht wijkt pseudonimiseren dus af van anonimiseren, waarbij de gegevens niet meer ontsleuteld kunnen worden. Het pseudonimiseren kan een nuttige methode zijn om een van de aspecten van proportionaliteit (zie hierna paragraaf 3.4) vorm te geven, namelijk ervoor te zorgen dat niet méér personen kennis nemen van de persoonsgegevens dan nodig is. Maar ook gepseudonimiseerde persoonsgegevens vallen onder de regels van de AVG. Ze zijn immers met toepassing van de sleutel te herleiden tot een individu. Alleen onomkeerbaar geanonimiseerde persoonsgegevens vallen buiten het bereik van de AVG.

Meer informatie over hoe binnen UWV wordt omgegaan met pseudonimiseren en anonimiseren is te vinden in de UWV Richtlijn Data Anonimisering en pseudonimisering (versie 1.1, 27-07-2018).

⁶ Dit geldt uiteraard alleen indien de aantallen waarover gerapporteerd wordt zodanig gekozen zijn dat een individu niet (meer) is te herleiden.

2.2. Wanneer is sprake van een verwerking?

Wat zegt de AVG?

Iedere bewerking van persoonsgegevens (bijv. de registratie van een nieuwe klant of medewerker) of van een geheel van persoonsgegevens (bijv. bewerkingen van een database met persoonsgegevens), wordt aangemerkt als een 'verwerking van persoonsgegevens'. Ook het enkele raadplegen of inzien van persoonsgegevens is een 'verwerking van persoonsgegevens'. Daarnaast valt onder de term 'verwerking van persoonsgegevens' het geheel van bewerkingen, zoals bijv. een bronsysteem of applicatie waarin persoonsgegevens worden verwerkt.

Met het begrip 'verwerking' wordt dus zowel de *handeling* die je met persoonsgegevens verricht bedoeld als het *systeem* of de *applicatie* waarin persoonsgegevens worden verwerkt.

Artikel 4 (2) AVG

In principe valt alles wat je met persoonsgegevens kan doen onder de definitie van 'verwerking van persoonsgegevens'. De AVG noemt een aantal voorbeelden van bewerkingen die hieronder worden besproken.

Het verzamelen en opvragen van persoonsgegevens

Het gaat hierbij bijvoorbeeld om gegevens die worden verzameld in het kader van een aanvraag voor een uitkering, in het kader van een sociaal-medische beoordeling of in het kader van de personeelsadministratie. Gegevens kunnen worden verzameld bij de betrokkene (deze vult een formulier in of wordt in een gesprek naar de gegevens gevraagd). Maar de gegevens kunnen ook bij derden worden opgevraagd.

Het inzien of raadplegen van persoonsgegevens

Alleen het bekijken of inzien van persoonsgegevens is al een verwerking van persoonsgegevens. Daarom is het van belang dat persoonsgegevens niet (kunnen) worden ingezien door een persoon, bijvoorbeeld een medewerker, als dit niet noodzakelijk is voor de taak van die persoon.

Het vastleggen, opslaan en bewaren van persoonsgegevens.

Het kan hierbij gaan om het vastleggen van persoonsgegevens in een fysiek dossier of in een digitaal dossier, in een systeem, database of applicatie. Het verzamelen van persoonsgegevens is dus al een verwerking die moet voldoen aan de eisen van de AVG. Ook alleen het bewaren van persoonsgegevens in een database is een verwerking onder de AVG.

Het gebruiken, bijwerken, wijzigen of aanvullen van persoonsgegevens.

Het gaat hier bijvoorbeeld om het gebruiken van persoonsgegevens om een werkplan op te stellen, een sociaal-medische beoordeling te doen of om een recht op uitkering vast te stellen. Maar het gaat ook om de persoonsgegevens van medewerkers die worden gebruikt in de personeelsadministratie om bijvoorbeeld salaris uit te betalen. Het vastleggen van een beoordeling in het personeelsdossier is ook een voorbeeld van de verwerking van persoonsgegevens.

Het ordenen, structureren, aligneren en combineren van persoonsgegevens.

Hieronder valt bijvoorbeeld het koppelen van bestanden met persoonsgegevens, het analyseren van persoonsgegevens en het profileren van personen op basis van persoonsgegevens. De werkzaamheden die onder de vlag van business intelligence of customer intelligence worden verricht vallen hieronder, voor zover dit niet op basis van onomkeerbaar geanonimiseerde gegevens gebeurt.

Het verstrekken, doorzenden, verspreiden, delen of ter beschikking stellen van persoonsgegevens.

Hieronder valt iedere handeling die ertoe leidt dat een ander toegang kan krijgen en kennis kan nemen van persoonsgegevens. Het doorgeven van een naam en adresgegevens van een klant aan een andere organisatie is dus een verwerking van persoonsgegevens.

Het afschermen, wissen of vernietigen van persoonsgegevens.

Een methode om persoonsgegevens af te schermen is het pseudonimiseren van persoonsgegevens. (zie ook paragraaf 2.1.3). Onder wissen of vernietigen van persoonsgegevens wordt hetzelfde verstaan. Het gaat daarbij

om het definitief verwijderen van persoonsgegevens uit de systemen van UWV. Zie voor dit onderwerp ook hoofdstuk 6 en paragraaf 9.3.

Ieder systeem, iedere applicatie, iedere database, ieder document en ieder proces waarvan UWV gebruikt maakt en waarin persoonsgegevens zijn opgenomen, moet dus worden beschouwd als een verwerking van persoonsgegevens. Maar ook het inzien, bewerken of verstrekken van bepaalde persoonsgegevens aan een derde valt onder het begrip 'verwerking'. Een verwerking kan dus duiden op een systeem of op een handeling.

2.3. Verwerkingsverantwoordelijke, verwerker en verwerkersovereenkomst

Wat zegt de AVG?

De AVG maakt onderscheid tussen 'verwerkingsverantwoordelijke' en 'verwerker'. Er gelden verschillende regels afhankelijk van de vraag of een organisatie persoonsgegevens verwerkt als verwerkingsverantwoordelijke of als verwerker.

De verwerkingsverantwoordelijke is de organisatie die het doel en de middelen voor de verwerking van persoonsgegevens vaststelt. Een verwerker is een organisatie die persoonsgegevens verwerkt ten behoeve van een verwerkingsverantwoordelijke. De verwerkingsverantwoordelijke moet ervoor zorgen dat er met de verwerker duidelijke afspraken zijn over privacybescherming, zoals bijvoorbeeld over de beveiliging van de gegevens. Deze afspraken moeten zijn vastgelegd in een verwerkersovereenkomst en de verwerkingsverantwoordelijke moet controleren of ze ook worden nagekomen.

Artikel 4 onder (7) en (8) en artikel 29 AVG

De AVG kent twee rollen waarin een organisatie persoonsgegevens kan verwerken: als verwerkingsverantwoordelijke of als verwerker.

Kort gezegd is de verwerkingsverantwoordelijke degene die bepaalt waarom en hoe de persoonsgegevens worden verwerkt. De verwerker is degene die ten behoeve van en in opdracht van de verwerkingsverantwoordelijke de persoonsgegevens verwerkt. Tussen verwerkingsverantwoordelijke en een verwerker moet een verwerkersovereenkomst zijn afgesloten.

Op enkele uitzonderingen na verwerkt UWV persoonsgegevens in de rol van verwerkingsverantwoordelijke.

Hoewel het onderscheid tussen verwerkingsverantwoordelijke en verwerker al bestond onder de oude Wet bescherming persoonsgegevens (Wbp) (toen werd de verwerker aangeduid als bewerker) is er met de invoering van de AVG extra aandacht gekomen voor dit onderscheid.

Het goed identificeren van de rol waarin de verwerking van persoonsgegevens plaatsvindt is van groot belang. De AVG koppelt aan elk van de rollen eigen verantwoordelijkheden en verplichtingen. Het onderscheid is belangrijk voor degene die de persoonsgegevens verwerkt; het is bepalend voor zijn verantwoordelijkheden en verplichtingen bij de verwerking van de persoonsgegevens en de afbakening daarvan ten opzichte van de partij waarmee hij samenwerkt. Het is echter ook belangrijk voor de betrokkene en de Autoriteit persoonsgegevens (AP) omdat het bepalend is voor de vraag wie zijn aanspreekpunt is bij de verwerking van persoonsgegevens.

Helaas is het in de praktijk niet altijd makkelijk te bepalen of een organisatie waarmee UWV samenwerkt zelf ook een verwerkingsverantwoordelijke of een verwerker is. Regelmatig bestaat dan ook onduidelijkheid over de vraag of een bedrijf of organisatie waarmee UWV zaken doet en die van UWV persoonsgegevens ontvangt, een verwerker is en of daarmee dan ook een verwerkersovereenkomst moet worden afsluiten. Ook omgekeerd wordt die vraag gesteld door bedrijven of organisaties die aan UWV persoonsgegevens verstrekken. Moeten zij met UWV een verwerkersovereenkomst sluiten? In deze paragraaf wordt getracht daarop in grote lijnen antwoord te geven. Indien in een samenwerkingsrelatie twijfel bestaat over de rollen van de betreffende organisaties, leg dan de casus voor aan de BSO van het eigen organisatieonderdeel en de privacyjuristen van Juridische Zaken.

2.3.1. Onderscheid tussen verwerkingsverantwoordelijke en verwerker

De AVG heeft de begrippen verwerkingsverantwoordelijke en verwerker gedefinieerd. Kort gezegd is een verwerkingsverantwoordelijke een organisatie die, alleen of samen met anderen, het doel ('waarom') en de middelen ('hoe') voor de verwerking van persoonsgegevens vaststelt. Een verwerker is kort gezegd een organisatie die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

Een verwerker maakt nooit onderdeel uit van de organisatie van de verwerkingsverantwoordelijke. Zo kan bijv. BKWI geen verwerker zijn van UWV omdat het een organisatieonderdeel van UWV is. BKWI werkt als een apart en herkenbaar organisatieonderdeel van UWV in opdracht van het Ministerie van Sociale Zaken en Werkgelegenheid. BKWI kan wel verwerker zijn voor andere verwerkingsverantwoordelijken.

Wanneer is een door UWV gecontracteerde leverancier verwerker? En wanneer zelf verwerkingsverantwoordelijke?

Om antwoord te geven op de vraag of een leverancier van UWV moet worden aangemerkt als een verwerker, is allereerst noodzakelijk dat er door de leverancier persoonsgegevens worden verwerkt in het kader van de door de leverancier aan UWV te leveren producten of diensten. Verwerkt de leverancier in dat kader geen persoonsgegevens, dan is de leverancier ten opzichte van UWV geen verwerker.

Echter, als de leverancier in het kader van de door hem aan UWV te leveren producten of diensten wel persoonsgegevens verwerkt, betekent dat nog niet automatisch dat de leverancier ook gekwalificeerd moet worden als verwerker.

Om als verwerker te worden gekwalificeerd is daarnaast nog noodzakelijk dat:

- de producten of diensten die de leverancier in opdracht UWV verricht gericht zijn op het verwerken van persoonsgegevens.
- de leverancier geen enkele zeggenschap heeft over de wijze waarop hij de persoonsgegevens verwerkt; die zeggenschap ligt bij UWV (de opdrachtgever/verwerkingsverantwoordelijke die doel en middelen van de verwerking bepaalt).

Als de gegevensverwerking door de leverancier een uitvloeisel (bijzaak) is van het leveren van zijn producten of diensten, dan is dat een indicatie dat er geen sprake is van een verwerker maar verwerkingsverantwoordelijke.

Voorbeelden van een leveranciersrelatie waarbij de leverancier verwerker is, zijn:

- het datacenter waarin de applicaties draaien waarmee UWV persoonsgegevens verwerkt en die ook zorgdraagt voor de digitale opslag van persoonsgegevens;
- het onderzoeksbureau dat in opdracht van UWV onderzoek verricht op basis van persoonsgegevens;
- de salarisadministrateur die ten behoeve van UWV de persoonsgegevens van de UWV-medewerkers verwerkt teneinde de salarisadministratie uit te voeren.

In deze voorbeelden behelst de kern van de dienst die de leverancier aan UWV levert het verwerken van persoonsgegevens. De leverancier verwerkt de persoonsgegevens ook geheel conform de instructies van UWV.

In het merendeel van de gevallen is de leverancier van UWV echter géén verwerker maar verwerkt hij de persoonsgegevens als verwerkingsverantwoordelijke die de persoonsgegevens heeft ontvangen omdat deze noodzakelijk zijn om zijn product of dienst te leveren. Voorbeelden van een leveranciersrelatie waarbij de leverancier zelf verwerkingsverantwoordelijke is, zijn:

- de leasemaatschappij die de leaseauto's van UWV verzorgt;
- Reisbalans, die die gegevens van UWV-medewerkers verwerkt voor de OV-kaart;
- de softwareleverancier van software die binnen UWV-omgeving draait,
- de bloemist waar UWV een bos bloemen besteld om aan een medewerker te leveren.

In deze voorbeelden behelst de kern van de opdracht immers niet de verwerking van persoonsgegevens. De leverancier verwerkt de persoonsgegevens alleen om zijn product of dienst te kunnen leveren. Het is ook niet UWV die het doel en de middelen bepaalt van de verwerking van de persoonsgegevens door de leverancier.

Wanneer is UWV in relatie tot derden verwerkingsverantwoordelijke? En wanneer verwerker?

Andersom komt het ook voor dat UWV werkzaamheden in samenwerking met of ten behoeve van derden verricht en daarvoor persoonsgegevens verwerkt. Ook hier kunnen vragen en misverstanden ontstaan over de rol waarin UWV de persoonsgegevens verwerkt. Is UWV verwerkingsverantwoordelijke of verwerker?

UWV als (gezamenlijke) verwerkingsverantwoordelijke

UWV verwerkt de persoonsgegevens ten behoeve van de uitvoering van de wettelijke taken als verwerkingsverantwoordelijke. Dat doet UWV namelijk niet in opdracht van de werkgever/werknemer/uitkeringsgerechtigde of namens de werkgever/werknemer/uitkeringsgerechtigde, maar voor de uitvoering van de eigen taak. UWV stelt doel en middelen van de verwerking vast. Er is dus geen sprake van dat UWV hierbij handelt als verwerker ten behoeve van de klant of een werkgever.

In samenwerkingsverbanden waarbij UWV samen met een andere organisatie een gezamenlijk doel nastreeft, zullen zowel UWV als de organisatie waarmee wordt samengewerkt in de regel beiden verwerkingsverantwoordelijke zijn. Bij de samenwerking van UWV met andere organisaties in het kader van de voorkoming en bestrijding van fraude, is bijvoorbeeld in de Wet SUWI bepaald dat samenwerkende organisaties gezamenlijke verwerkingsverantwoordelijken zijn.⁷

Bij de regionale samenwerking van UWV en gemeenten als bedoeld in artikel 10 van de Wet SUWI is bepaald dat UWV en de gemeente bij die samenwerking gezamenlijke verwerkingsverantwoordelijken zijn voor de verwerking van persoonsgegevens voor de uitvoering van taken op grond van onder meer de WW, de AG-wetten en de Participatiewet ten aanzien van dezelfde uitkeringsgerechtigde of werkzoekende⁸. In hoeverre daarvan in een concreet geval sprake is, wordt nader beschreven in een (nog op te stellen) beleidsdocument.

Er is in deze voorbeelden geen sprake van een verwerkingsverantwoordelijke – verwerker relatie.

UWV als verwerker

Voor sommige verwerkingen is in de wet bepaald dat UWV 'verwerker' is. Het gaat bijvoorbeeld om de verwerking van bepaalde gegevens in de polisadministratie (zie artikel 33 lid 3 Wet SUWI).⁹ Voor die gegevens is de Belastingdienst of het CBS verwerkingsverantwoordelijke en UWV verwerker.

Bij het uitvoeren van de zogenaamde andere werkzaamheden (als bedoeld in artikel 5 Wet SUWI) kan de situatie ontstaan dat UWV bij het uitvoeren van die werkzaamheden ten behoeve van de opdrachtgever persoonsgegevens verwerkt in de rol van verwerker ten behoeve van de opdrachtgever die verwerkingsverantwoordelijke is. Dat is echter alleen het geval als voldaan is aan de hierboven omschreven voorwaarden die worden gebruikt om de leverancier (in dit geval dan UWV) te kunnen kwalificeren als verwerker.

2.3.2. Eisen die gelden voor de relatie verwerkingsverantwoordelijke – verwerker

De AVG stelt een aantal eisen aan de relatie verwerkingsverantwoordelijke – verwerker (zie artikel 28 AVG). Kort gezegd betekent dit voor UWV het volgende:

- Voordat met een verwerker in zee wordt gegaan, moet UWV onderzoek doen naar de desbetreffende organisatie om zich ervan te verzekeren dat de organisatie in staat is aan de AVG-eisen te voldoen.
- Met de verwerker moet UWV een schriftelijke verwerkersovereenkomst afsluiten waarin een aantal belangrijke verplichtingen van de verwerker worden vastgelegd. (zie hierna)
- UWV moet schriftelijke instructies opstellen waaraan de verwerker zich moet houden.
- UWV moet periodiek controles of inspecties uitvoeren bij de verwerker om na te gaan of de verwerker zich aan de afspraken en instructies houdt.
- De verwerker mag alleen na voorafgaande goedkeuring van UWV een andere organisatie in de arm nemen dat een deel van zijn werkzaamheden verricht met de persoonsgegevens van UWV.

De verwerkersovereenkomst

Indien er sprake is van een relatie UWV – verwerker stelt de AVG de eis dat er tussen verwerkingsverantwoordelijke en verwerker een schriftelijke verwerkersovereenkomst wordt gesloten. De AVG schrijft voor wat er minimaal in de verwerkersovereenkomst geregeld moet zijn. Naast de bepaling dat de verwerker de persoonsgegevens uitsluitend verwerkt op basis van schriftelijke instructies van de verwerkingsverantwoordelijke, moeten in de verwerkersovereenkomst ook zijn opgenomen verplichtingen voor de verwerker op het terrein van beveiliging, geheimhouding, melden van datalekken, medewerking verlenen aan verzoeken van betrokkenen (bijv. verwijdering van gegevens) en aan onderzoek van de Autoriteit Persoonsgegevens, en het verwijderen/vernietigen van de gegevens na einde van de overeenkomst.¹⁰

⁷ Artikel 64 lid 2 Wet SUWI

⁸ Artikel 62 lid 3 Wet Suwi

⁹ Gegevens betreffende genoten loon, ingehouden loonbelasting, premie volksverzekeringen en gegevens van de werknemer die van belang zijn voor statische doeleinden op het gebied van arbeid en loon. (artikel 33 lid 2 (d) en (d) Wet SUWI)

¹⁰ Zie artikel 28 lid 3 AVG.

De verwerkersovereenkomst kan een aparte overeenkomst zijn maar mag ook onderdeel zijn van een meer omvattende overeenkomst. Bij het afsluiten van contracten met leveranciers wordt, indien ook beveiligingsaspecten aan de orde zijn, gebruik gemaakt van BVO's (Beveiligings- en Verwerkersovereenkomsten). In het format van de BVO is een onderdeel opgenomen dat – in het geval dat de leverancier wordt aangemerkt als verwerker – kan dienen als verwerkersovereenkomst. Daarnaast bestaat ook een format voor een 'losse' verwerkersovereenkomst.

In het geval er geen relatie verwerkingsverantwoordelijke – verwerker is (dus zowel UWV als de leverancier zijn beiden verwerkingsverantwoordelijke), wordt er géén verwerkersovereenkomst gesloten. Zou dat wel gebeuren, dan wordt er een relatie benoemd die er niet is met alle gevolgen van dien (zoals verwarring over wie er nu verantwoordelijk is als er bij de verwerking van persoonsgegevens door de leverancier iets mis gaat).

Dat een leverancier in de relatie met UWV de rol van verwerkingsverantwoordelijke heeft en UWV en de leverancier dus geen verwerkersovereenkomst sluiten, betekent geenszins dat de leverancier met de voor het uitvoeren van de opdracht ontvangen persoonsgegevens kan doen en laten wat hij wil. De leverancier is namelijk als verwerkingsverantwoordelijke zelf ook volledig gebonden aan de AVG. Daarnaast kan UWV aan de leverancier eisen stellen over de omgang met en de beveiliging van de persoonsgegevens (zolang die afspraken er maar niet toe leiden dat UWV doel en middelen van de verwerking bepaalt en zolang het ook maar geen verwerkersovereenkomst wordt genoemd).

2.4. UWV beleidskader algemene begrippen

- **UWV verwerkt veel gegevens die onder de definitie van persoonsgegevens vallen en deze verwerkingen moeten dus aan de AVG voldoen. Het gaat bijvoorbeeld om alle informatie over of gerelateerd aan klanten, medewerkers, bezoekers (van gebouwen, maar ook van portalen en websites), personen die UWV inhuurt of die aan UWV diensten verlenen.**
- **Ook gepseudonimiseerde gegevens zijn persoonsgegevens die onder de AVG vallen.**
- **Alleen wanneer persoonsgegevens onomkeerbaar geanonimiseerd worden is geen sprake meer van persoonsgegevens in de zin van de AVG. Op de verdere verwerking van deze anonieme gegevens zijn de regels van de AVG dan ook niet van toepassing. De drempel om van onomkeerbaar geanonimiseerde persoonsgegevens te spreken ligt hoog. Omdat UWV over een zeer grote hoeveelheid persoonsgegevens beschikt, zal – zeker in de analyseomgevingen – veelal niet kunnen worden gesteld dat sprake is van onomkeerbaar geanonimiseerde persoonsgegevens.**
- **Gegevens die op geaggregeerd niveau zijn weergegeven en niet meer te herleiden zijn tot een individu, zijn geanonimiseerd. Maar de analyses die vooraf zijn gegaan aan het opstellen van zo'n rapportage zijn in veruit de meeste gevallen verwerkingen van persoonsgegevens.**
- **Alle vormen van bewerkingen van persoonsgegevens zijn verwerkingen in de zin van de AVG. Ook het enkele verzamelen (waaronder ontvangen), bewaren, inzien of raadplegen van persoonsgegevens is een verwerking van persoonsgegevens in de zin van de AVG.**
- **De meeste systemen, applicaties en databases waarin UWV persoonsgegevens verwerkt, zijn verwerkingen van persoonsgegevens in de zin van de AVG.**
- **De verwerking van deze persoonsgegevens moet voldoen aan de AVG, UAVG en andere relevante wetgeving (zoals de Wet SUWI, de Wet BIG, de Archiefwet), de beleidsregels van de Autoriteit Persoonsgegevens, dit beleidskader, overig Informatiebeveiligings- en privacybeleid en instructies van UWV.**
- **Behoudens enkele uitzonderingen verwerkt UWV persoonsgegevens in de hoedanigheid van verwerkingsverantwoordelijke.**
- **Een verwerker in de zin van de AVG is een organisatie die persoonsgegevens verwerkt ten behoeve van een verwerkingsverantwoordelijke. Het enkele feit dat een leverancier een opdracht ten behoeve van UWV uitvoert en daarbij persoonsgegevens van UWV ontvangt betekent nog niet**

dat de leverancier verwerker is. Ook het feit dat een organisatie (zoals bijv. een werkgever) aan UWV persoonsgegevens verstrekt betekent niet dat UWV verwerker is.

- Indien er sprake is van een verwerkingsverantwoordelijke – verwerkers relatie, dan moet er tussen de verwerkingsverantwoordelijke en de verwerker een verwerkersovereenkomst worden gesloten die voldoet aan de eisen die de AVG daaraan stelt. UWV gebruikt hiervoor in de relatie met leveranciers het model van de Beveiligings- en verwerkersovereenkomst (BVO) of een ander format van een verwerkersovereenkomst. UWV zorgt voor schriftelijke instructies inzake de verwerking van persoonsgegevens en ziet toe op de naleving daarvan en van de contractueel vastgelegde afspraken door het periodiek uitvoeren van audits of inspecties.**
- Is de leverancier geen verwerker in de zin van de AVG, dan moet er géén verwerkersovereenkomst worden gesloten.**

3. Beginselen die gelden voor alle verwerkingen van persoonsgegevens

De AVG kent een aantal beginselen die *altijd* in acht moeten worden genomen wanneer een organisatie persoonsgegevens wil verwerken. Deze beginselen gelden daarom voor alle verwerkingen van UWV. In de volgende paragrafen worden de beginselen besproken. Daarbij wordt ook ingegaan op de vraag wat deze beginselen voor UWV betekenen.

3.1. De verwerking moet rechtmatig zijn

Wat zegt de AVG?

De verwerking van persoonsgegevens mag alleen plaatsvinden als deze rechtmatig is, dat wil in dit verband zeggen als hiervoor een grondslag bestaat. Er zijn zes grondslagen voor een rechtmatige verwerking van persoonsgegevens. Deze worden in hoofdstuk 4 besproken. Is geen van deze zes grondslagen aanwezig, dan is de verwerking onrechtmatig.

Artikel 5 lid 1 (a) en artikel 6 AVG

Dit betekent hier dat van iedere verwerking van persoonsgegevens bij UWV duidelijk moet zijn op welke van de zes grondslagen de verwerking is gebaseerd. In hoofdstuk 4 wordt meer in detail ingegaan op de grondslagen die voor UWV van betekenis zijn. De grondslag voor iedere verwerking moet worden toegelicht in de privacyverklaring (paragraaf 8.1) en vastgelegd in het register van verwerkingen (paragraaf 8.2).

Het beginsel dat de verwerking rechtmatig moet zijn, houdt tevens in dat als ook andere regelgeving van toepassing is, de verwerking ook daaraan moet voldoen. Een voorbeeld hiervan is dat de verwerking van medische gegevens door een verzekeringsarts ook moet voldoen aan de eisen die volgen uit de Wet geneeskundige behandelingsovereenkomst en de Wet op de beroepen in de individuele gezondheidszorg (Wet BIG). Een ander voorbeeld betreft het gebruik van cookies en andere technieken om het online-gedrag van klanten vast te leggen. Dit dient bijvoorbeeld ook aan de eisen van de Telecommunicatiewet te voldoen.

Het is van belang bij nieuwe verwerkingen vooraf de grondslag vast te stellen in een gegevensbeschermingseffectbeoordeling (GEB) (zie ook paragraaf 11.1). Ontbreekt een grondslag voor de verwerking, dan is deze onrechtmatig en moet de verwerking worden gestaakt.

3.2. De verwerking moet behoorlijk en transparant zijn

Wat zegt de AVG?

De verwerking van persoonsgegevens mag alleen plaatsvinden als dit behoorlijk en transparant is ten opzichte van de persoon van wie gegevens worden verwerkt.

Artikel 5 lid 1 (a) AVG

Als een organisatie persoonsgegevens verwerkt moet die verwerking behoorlijk en transparant zijn.

Bij de vraag of een verwerking 'behoorlijk' is, speelt een rol of de verwerking maatschappelijk geaccepteerd is en in lijn is met wat de betrokkene in redelijkheid kon verwachten. Wanneer UWV bijvoorbeeld besluit de inhoud van al het berichten- en telefoonverkeer van medewerkers vanuit de werkplekomgeving te monitoren, ook als het om privéberichten en persoonlijke gesprekken gaat, wordt dit ook als onbehoorlijk beschouwd. Het ligt niet in de lijn der verwachting dat UWV zich op deze wijze met het privéleven van medewerkers bemoeit. Ook als

UWV klantgegevens zou verkopen aan derde partijen, zou dit een verwerking zijn die niet aansluit bij wat burgers van UWV verwachten. Een dergelijke verwerking zou daarom al snel als onbehoorlijk worden gekwalificeerd.

Een verwerking is 'transparant' als voor de betreffende persoon duidelijk is dat een organisatie diens persoonsgegevens verwerkt, welke persoonsgegevens dat zijn en voor welke doel. Alleen dan kan de betrokkene controle houden over zijn gegevens en zijn rechten - bijvoorbeeld het recht op inzage - uitoefenen.

Het beginsel van transparantie geldt voor UWV niet alleen ten opzichte van onze klanten, maar ook ten opzichte van de medewerkers en andere relaties. Ook voor hen moet duidelijk zijn voor welke doelen en op welke grondslag UWV hun persoonsgegevens verwerkt.

In hoofdstuk 8 wordt meer in detail ingegaan op de eisen van transparantie en de wijze waarop UWV hieraan vorm geeft.

3.3. De verwerking moet voldoen aan het beginsel van doelbinding

Wat zegt de AVG?

Persoonsgegevens mogen alleen worden verwerkt voor een duidelijk omschreven en gerechtvaardigd doel. Ze mogen alleen voor een ander doel dan het oorspronkelijke doel worden verwerkt, als dat andere doel verenigbaar is met het oorspronkelijke doel.

Artikel 5 lid 1 (b) AVG

Voor elke verwerking moet vooraf duidelijk zijn welk doel met de verwerking wordt nagestreefd. Dit doel moet duidelijk omschreven zijn en moet worden vastgelegd in het register van verwerkingen. (zie paragraaf 8.2) Het doel van de verwerking is nauw verweven met de andere AVG-beginselen. Welke gegevens je gaat verwerken, welke medewerkers daar toegang tot moeten hebben en hoe lang je de gegevens bewaart, hangt allemaal af van het verwerkingsdoel dat je vooraf hebt bepaald. Het is daarom van belang dat het doel van de verwerking goed is vastgesteld.

Gegevens die zijn verkregen voor een bepaald doel, mogen vervolgens niet zomaar worden gebruikt voor een ander doel. Dit is alleen toegestaan als aan bepaalde voorwaarden wordt voldaan. Het beginsel van doelbinding voorkomt zo dat organisaties persoonsgegevens die zij hebben verzameld als hun eigendom zien waarmee ze naar eigen inzicht kunnen doen wat ze willen. Wil een organisatie verkregen persoonsgegevens verder verwerken voor een nieuw doel, dan zijn hiervoor drie mogelijkheden.

De eerste mogelijkheid is dat de betrokkene uitdrukkelijke toestemming geeft voor de nieuwe verwerking. De betrokkene moet dan vooraf zijn geïnformeerd over de doeleinden van de nieuwe verwerking en over zijn rechten, waaronder het recht om bezwaar te maken tegen de verdere verwerking.

Zoals in paragraaf 4.6 zal worden toegelicht is het voor UWV niet eenvoudig om op basis van toestemming te werken. Dit komt doordat klanten en medewerkers een afhankelijkheidspositie hebben ten opzichte van UWV. Toestemming kan daardoor bijna nooit vrijelijk worden gegeven en dit is een voorwaarde om van toestemming gebruik te kunnen maken. Verdere verwerking op grond van toestemming is daarom voor UWV niet aannemelijk en wanneer een organisatieonderdeel dit overweegt moet altijd vooraf het advies van de privacyjuristen van JZ worden ingewonnen.

Verdere verwerking van gegevens voor een nieuw doel is ook mogelijk als in de wet is vastgelegd dat dit voor een specifieke taak en doeleinde als rechtmatig en verenigbaar moet worden beschouwd. Dit kan aan de orde zijn bij een verwerking die belangrijke doelstellingen van algemeen belang moet waarborgen of bij een taak in het kader van de uitoefening van openbaar gezag. Het is ook hier van groot belang dat aan de andere beginselen van de AVG wordt voldaan en dat betrokkene vooraf over de verdere verwerking en het doeleinde daarvan wordt geïnformeerd, als ook over zijn rechten, zoals het recht om bezwaar te maken tegen deze

verdere verwerking.¹¹

Voor UWV geldt dat in de Wet SUWI ruimte is gecreëerd om gegevens die zijn verkregen voor de uitvoering van de ene wettelijke taak ook voor de uitvoering van een andere wettelijke taak te gebruiken. Hiertoe moet dan wel in een algemene maatregel van bestuur zijn vastgelegd welke gegevens kunnen worden gebruikt voor de uitvoering van de andere werkzaamheden en kunnen regels worden gesteld voor de wijze waarop de gegevensverstrekking plaatsvindt.¹²

Ten slotte kan een organisatie zelf een beoordeling maken en daarmee verantwoorden dat de verdere verwerking verenigbaar is met het oorspronkelijke doel van verwerking. Bij de beoordeling van deze verenigbaarheid, moet met een aantal aspecten rekening worden gehouden.¹³ Deze zijn:

- Is er een duidelijk verband tussen het oorspronkelijke doel en het nieuwe doel? Hoe groter het verband tussen het oorspronkelijke doel en het nieuwe doel van de verwerking, hoe eerder sprake zal zijn van een verenigbaar doel.
- Kan de betrokkene redelijkerwijs verwachten dat de gegevens voor het andere doel worden gebruikt? Zo nee, dan zal minder snel kunnen worden aangenomen dat de verdere verwerking verenigbaar is met het oorspronkelijke doel.
- Gaat het om gebruik van bijzondere persoonsgegevens (bijv. gezondheidsgegevens) of gegevens van strafrechtelijke aard, dan zal extra kritisch moeten worden gekeken naar het nieuwe doel en de vraag of verdere verwerking verenigbaar is met het oorspronkelijke doel.
- Heeft de verdere verwerking negatieve gevolgen voor de betrokkene? Zo ja, dan zal minder snel mogen worden aangenomen dat de verdere verwerking verenigbaar is met het oorspronkelijke doel.
- Zijn er passende waarborgen getroffen, zoals uitgebreide beveiligingsmaatregelen of maatregelen die de negatieve gevolgen (volledig) weg kunnen nemen?? Zo nee, dan moet extra kritisch worden gekeken naar de vraag of de verdere verwerking verenigbaar is met het oorspronkelijke doel.

In een aantal situaties wordt verenigbaarheid door de aard van de verwerking in de AVG verondersteld. Dit is het geval bij de verdere verwerking van gegevens met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of (uitsluitend) statistische doeleinden. Natuurlijk moeten deze verwerkingen ook voldoen aan de andere beginselen en dus bijvoorbeeld proportioneel zijn. Ook worden er in die situaties extra hoge eisen gesteld aan de beveiliging van de persoonsgegevens, bijvoorbeeld door het pseudonimiseren van de persoonsgegevens.¹⁴

Wanneer het nieuwe doel van de verwerking verenigbaar is met het oorspronkelijke doel is er geen afzonderlijke grondslag voor de verwerking van deze gegevens vereist: deze blijft dan gelijk aan de grondslag op basis waarvan de gegevens oorspronkelijk zijn verkregen.¹⁵

Bij UWV worden veel gegevens verzameld die voor verschillende taken worden ingezet. Dit is een bewuste keuze van UWV omdat UWV betrokkenen niet steeds om dezelfde gegevens wil hoeven vragen. Gegevens die bij een WW-aanvraag zijn verzameld, worden bijvoorbeeld ook voor re-integratie of handhaving gebruikt. Om aan het beginsel van doelbinding te voldoen moet UWV, voordat het gegevens voor een andere taak inzet, altijd eerst vaststellen of die nieuwe taak onder hetzelfde doel valt als waarvoor de gegevens verzameld zijn. Of, als het een ander doel betreft, dat dit nieuwe doel op basis van de criteria verenigbaar is met het oorspronkelijke doel of dat in een algemene maatregel van bestuur is vastgelegd dat het gegeven voor het nieuwe doel gebruikt mag worden.

Het vaststellen van doelbinding is een van de onderdelen in een Gegevensbeschermingseffectbeoordeling (ook wel GEB, zie paragraaf 11.1). Wanneer doelbinding is gebaseerd op verenigbaarheid met het oorspronkelijke doel, dan moet deze verenigbaarheid aan de hand van bovengenoemde aspecten worden onderbouwd en in het GEB-rapport worden vastgelegd.

¹¹ Artikel 6 lid 4 AVG en Overweging 50 AVG

¹² Artikel 73 a lid 1 Wet SUWI

¹³ Zie artikel 6 lid 4 AVG.

¹⁴ Overweging 50 AVG

¹⁵ Overweging 50 AVG

3.4. Er moet sprake zijn van minimale en proportionele gegevensverwerking

Wat zegt de AVG?

De verzameling en verwerking van persoonsgegevens moet zich beperken tot die persoonsgegevens die relevant en noodzakelijk zijn voor het doel van de verwerking. De verwerking van persoonsgegevens moet proportioneel zijn, dat wil zeggen in redelijke verhouding staan tot het doel van de verwerking.

Artikel 5 lid1 (c) AVG

Proportionaliteit betekent dat organisaties niet méér gegevens mogen verzamelen, gebruiken en verstrekken dan noodzakelijk is voor het specifieke doel van de verwerking. Dit zou namelijk disproportioneel zijn en daarmee onrechtmatig. Dit beginsel houdt ook in dat de verwerking van persoonsgegevens in redelijke verhouding moet staan tot het doel van de verwerking. Hierbij moet niet alleen worden gekeken naar de omvang van de gegevens, maar ook naar de aard van de gegevens (gaat het bijvoorbeeld om extra gevoelige gegevens, zoals gezondheidsgegevens). Wanneer de gegevens van een bepaalde groep uitkeringsgerechtigden bijvoorbeeld worden verstrekt voor een doel dat slechts een enkeling daarvan dient, zal die verstrekking als niet proportioneel moeten worden aangemerkt.

Minimale gegevensverwerking houdt ook verband met het beginsel van subsidiariteit. Dit beginsel houdt in dat je bij de verwerking van persoonsgegevens moet nagaan of er alternatieven zijn om het doel te bereiken die minder ingrijpend zijn voor de betrokkene. Is dit het geval, bijvoorbeeld omdat het mogelijk is een bepaalde rapportage ook op te stellen door gebruik te maken van geanonimiseerde gegevens, dan zal daarvoor moeten worden gekozen.

Minimale gegevensverwerking geldt ook bij de verstrekking van persoonsgegevens binnen UWV tussen collega's. Bedenk wat de ander nodig heeft en geef niet meer dan dat. Als bijvoorbeeld de bedrijfsarts voor een zieke medewerker tijdelijk een parkeerplaats nodig acht, dan heeft facilitair bedrijf (FB) niet méér gegevens nodig dan de naam van de medewerker en de periode dat een parkeerplaats nodig is. De reden van de aanvraag is privacygevoelig en heeft FB niet nodig. Wanneer je een verzendbestand wil exporteren, exporteer dan alleen de naam en het e-mailadres en niet andere gegevens die in het systeem staan en niet nodig zijn voor de verzending. Wanneer een vraag of klacht van een klant binnenkomt bij K&S en wordt doorgezet naar iemand binnen een van de organisatieonderdelen, kijk dan kritisch of het voor beantwoording van de vraag nodig is om naam, e-mail en BSN door te sturen. Zo niet, dan vraagt het beginsel van dataminimalisatie dat die gegevens niet worden meegestuurd.

Tenslotte is het beginsel van minimale gegevensverwerking ook van belang als het gaat om de vraag wie toegang heeft tot persoonsgegevens en voor welke duur. Uitgangspunt zou moeten zijn dat iedere medewerker alleen bij die persoonsgegevens kan die hij of zij nodig heeft voor zijn taken. En dan alleen voor de duur dat hij of zij die taken met betrekking tot die specifieke zaak¹⁶ van een klant uitvoert. Wanneer de zaak is afgehandeld zou de medewerker geen toegang meer moeten hebben tot de gegevens. Dit zou via privacy by design en autorisatiebeheer moeten worden afdgedwongen.

Hoeveel en welke medewerkers een taak hebben in een zaak is afhankelijk van de inrichting van de bedrijfsvoering. Er zijn processen waarin een klein team van een contactpersoon, een ondersteuner en een vervanger de zaak van een klant afhandelen. De toegang tot de persoonsgegevens van de klant die voor deze zaak nodig zijn kan dan beperkt blijven tot dit kleine team. Er zijn echter ook situaties waarbij er geen vaste klant-medewerker relatie bestaat, en de taken voor een bepaalde zaak al naar gelang het moment bij iedereen van een bepaalde afdeling kunnen worden ingedeeld. In die situaties is het voor de continuïteit van de dienstverlening van belang dat een medewerker op het moment dat hij de taak toebedeeld krijgt toegang heeft tot die gegevens van de betreffende klant die nodig zijn voor het uitvoeren van de taak. Soms betekent dit in de praktijk dat de hele afdeling toegang tot de gegevens krijgt. Het proportionaliteitsbeginsel vergt echter dat wordt

¹⁶ *Zaakgericht werken is een manier van werken die zich richt op het goed en transparant afhandelen van 'zaken.' Een zaak is in dit verband een samenhangende hoeveelheid werk, met een duidelijke aanleiding en een duidelijk resultaat";* definitie zaakgericht werken Nederlandse Overheid Referentie Architectuur (NORA) Binnen UWV wordt geleidelijk het project Werken met Zaken (onderdeel van E-werken) uitgerold. Dit is een belangrijke stap in het verder richting het AVG-proof werken binnen UWV.

nagestreefd de groep medewerkers die toegang heeft tot persoonsgegevens van een klant of andere betrokkene zo beperkt mogelijk te houden. Dit betekent dat bij de inrichting van de bedrijfsvoering goed moet worden nagedacht hoe zowel continuïteit als proportionaliteit kan worden gewaarborgd. (zie ook privacy by design in paragraaf 3.8)

Concluderend: bij iedere (voorgenomen) verwerking moet dus kritisch worden gekeken naar welke gegevens écht nodig zijn voor het desbetreffende doel en moet voorkomen worden dat méér dan die gegevens worden verzameld, vastgelegd, gebruikt en/of verstrekt of voor een langere duur dan noodzakelijk voor het desbetreffende doel.

Voor de toepassing van dit beginsel zijn de volgende vragen steeds van belang:

- Staat de verwerking (waaronder ook de verstrekking) van de persoonsgegevens in redelijke verhouding tot het doel dat de verwerking dient?
- Worden niet méér gegevens verzameld, gebruikt of verstrekt dan noodzakelijk voor het doel? Kan het beoogde doel bijvoorbeeld ook worden bereikt door geanonimiseerde gegevens te gebruiken? Indien bijzondere persoonsgegevens of het BSN worden verwerkt, kan het beoogde doel ook zonder deze gegevens worden bereikt?
- Kunnen alleen die medewerkers de persoonsgegevens raadplegen en gebruiken die deze ook daadwerkelijk nodig hebben om hun taak uit te voeren?
- Is de toegang van deze medewerkers tot de gegevens beperkt tot de duur dat zij deze gegevens nodig hebben voor de betreffende zaak van de betrokkene?

3.5. De persoonsgegevens die worden verwerkt moeten correct zijn

Wat zegt de AVG?

Een organisatie die persoonsgegevens verwerkt moet ervoor zorgen dat de persoonsgegevens correct zijn en up-to-date worden gehouden. Maatregelen moeten worden getroffen om onjuiste gegevens te corrigeren of te wissen.

Artikel 5 lid 1 (d) AVG

Dit betekent dat er tot op zekere hoogte op UWV een plicht rust om ervoor te zorgen dat de gegevens die UWV verwerkt correct zijn én blijven. Dit geldt ook en misschien wel juist voor adresgegevens. Foutieve of verouderde adressen kunnen er gemakkelijk toe leiden dat – soms gevoelige – persoonsgegevens bij de verkeerde persoon terecht komen. Dit kan dan leiden tot een datalek (zie paragraaf 11.2). Het is daarom van belang dat de organisatieonderdelen bij de verwerking van persoonsgegevens technische en organisatorische maatregelen treffen om ervoor te zorgen dat de gegevens zo actueel mogelijk zijn. Data Office (Gegevensdiensten) heeft meerdere beleidstukken op het gebied van datakwaliteit die onder andere de compleetheid, accuraatheid en actualiteit van gegevens beschrijft en handvatten geeft voor het controleren en verbeteren van de kwaliteit (zie ook de bijlage).¹⁷

Specifiek bij het actueel houden van het adressenbestand van de klanten van UWV spelen de implementatie van het adressenbeleid (*Uitvoeringsbeleid Adressen op burgerservicenummer niveau, 12 november 2019*) en de UWV Personenadministratie (UPA) een belangrijke rol.

Tegelijkertijd hebben de klanten van UWV ook de plicht om UWV op de hoogte te stellen van alle informatie die relevant is in verband met hun uitkering. Zie bijvoorbeeld de artikelen 27 Wet WIA, 49 ZW en 2.7 Wet Wajong. Op grond hiervan wordt ook van onze klanten verwacht dat zij zelf bijdragen aan het actueel houden van hun gegevens. Maar deze informatieplicht betekent niet dat UWV achterover kan leunen. UWV moet het de klant zo makkelijk mogelijk maken om wijzigingen in gegevens door te geven, maar ook bij de klant de juistheid van de gegevens controleren. Ook moet UWV er zelf voor zorgen dat de eigen mogelijkheden, zoals adresverificatie in de basisregistratie personen, zo goed mogelijk worden benut. Daarnaast is het van belang dat in de verschillende processen wordt beschreven hoe de relevante persoonsgegevens actueel worden gehouden.

¹⁷ Zie de DWU overzichtspagina Data Office UWV Producten en Kaders:
<https://digitalewerkplek.sharepoint.uwv.nl/uwv/organisatieonderdelen/Paginas/DataOfficeUWVProductenKaders.aspx>

Als de gegevens onjuist zijn, kunnen betrokkenen ook officieel verzoeken om correctie van de gegevens. Zie hiervoor paragraaf 9.2.

Voor de toepassing van dit beginsel is de volgende vraag van belang:

- Hoe wordt ervoor gezorgd dat de persoonsgegevens juist en actueel zijn én blijven?

3.6. De bewaartermijn van de persoonsgegevens moet zo beperkt mogelijk zijn

Wat zegt de AVG?

Persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk is voor het doel waarvoor ze worden verwerkt. Als de persoonsgegevens niet meer nodig zijn voor het doel waarvoor ze zijn verwerkt, moeten ze dus worden vernietigd, tenzij er een andere wet is, zoals de Archiefwet, die de organisatie verplicht tot het langer bewaren van die gegevens.

Artikel 5 lid 1 (e) AVG

Uitgangspunt van de AVG is dat persoonsgegevens niet langer mogen worden bewaard dan noodzakelijk voor het doel waarvoor ze worden verwerkt. Dit betekent dat wanneer een dossier of een (verzekerings)zaak is afgesloten of een procedure is afgerond - bijv. een uitkeringsgerechtigde ontvangt niet langer een uitkering en/of een bezwaarprocedure is afgerond - de gegevens op grond van de AVG in principe vernietigd moeten worden. UWV is echter een overheidsorganisatie die zich richting burgers en overheid dient te verantwoorden over zijn handelen. Dit is vastgelegd in de Archiefwet, die ook op UWV van toepassing is. Daarom moeten gegevens ook na afsluiting van een zaak nog een bepaalde termijn beschikbaar blijven. Hoe lang deze termijn voor een bepaald gegeven is, is opgenomen in de Selectielijst UWV.¹⁸ Aan het einde van die bewaartermijn worden – afhankelijk van de status - de desbetreffende gegevens vernietigd of overgebracht naar het Nationaal Archief.

Gelet op het beginsel van doelbinding, is het uitgangspunt dat op het moment dat het lopende dossier is afgerond, de persoonsgegevens niet meer voor medewerkers toegankelijk zijn. De gegevens vallen vanaf dat moment onder het regime van de Archiefwet en kunnen in beginsel alleen met toestemming van de voor het archief verantwoordelijk - dit is bij UWV Hoofd DIV - worden geraadpleegd.

Voor de toepassing van dit beginsel zijn de volgende vragen steeds van belang:

- Is duidelijk hoe lang de persoonsgegevens die worden verwerkt mogen/moeten worden bewaard?
- Hoe is geregeld dat de persoonsgegevens na het verstrijken van de bewaartermijn worden vernietigd?

In hoofdstuk 6 wordt meer in detail ingegaan op het opslaan, archiveren en vernietigen van persoonsgegevens.

¹⁸ Staatscourant 2017, nr. 9044.

3.7. De persoonsgegevens moeten adequaat zijn beveiligd

Wat zegt de AVG?

Persoonsgegevens moeten worden beveiligd zodat de integriteit en vertrouwelijkheid daarvan is gewaarborgd. Organisaties die persoonsgegevens verwerken moeten daarom passende technische en organisatorische maatregelen nemen zodat de gegevens zijn beschermd tegen ongeoorloofde of onrechtmatige verwerking of tegen onopzettelijk verlies, vernietiging of beschadiging.

Artikel 5 lid 1 (f) en artikel 32 AVG

Bij de verwerking van persoonsgegevens is het van belang de beschikbaarheid, integriteit en vertrouwelijkheid van de gegevens te waarborgen. Onder 'beschikbaarheid' wordt verstaan dat de gegevens kunnen worden geraadpleegd en/of gebruikt op het moment dat dat voor een bepaalde taak nodig is. Onder 'integriteit' van persoonsgegevens wordt verstaan dat de persoonsgegevens volledig en juist zijn gedurende het gehele proces van verwerking en dat dit onomstotelijk kan worden vastgesteld. Onder 'vertrouwelijkheid' van persoonsgegevens wordt verstaan dat de persoonsgegevens alleen toegankelijk zijn voor personen die bevoegd zijn ervan kennis te nemen en dus voor andere zijn afgeschermd. Hierdoor kan ook worden voorkomen dat de gegevens onbevoegd worden gewijzigd. Door middel van het nemen van technische en organisatorische beveiligingsmaatregelen kunnen de beschikbaarheid, integriteit en vertrouwelijkheid van persoonsgegevens worden gewaarborgd.

Wie persoonsgegevens verwerkt, moet er daarom voor zorgen dat die persoonsgegevens voldoende zijn beveiligd tegen ongeoorloofde of onrechtmatige verwerking of tegen onopzettelijk verlies, vernietiging of beschadiging. Onder ongeoorloofde verwerking wordt ook verstaan de ongeoorloofde inzage of kennisneming van die gegevens. Dit betekent dat ook maatregelen moeten worden getroffen om te voorkomen dat medewerkers toegang hebben tot persoonsgegevens die deze niet nodig hebben voor hun specifieke taken, zoals autorisatiebeheer.

Omdat UWV over zeer veel gevoelige persoonsgegevens beschikt die ook voor (criminele) derden interessant zijn, is ook de technische beveiliging van onze systemen van zeer groot belang. Grote databestanden met persoonsgegevens zijn veel geld waard voor datahandelaren. Met de combinatie van naam, BSN en bankrekeningnummer kunnen criminelen bijvoorbeeld identiteitsfraude plegen en informatie over de hoogte van het inkomen kan misbruikt worden voor de mogelijke afpersing van een persoon. Er zijn ook voorbeelden dat uitkeringsgerechtigden slachtoffer zijn geworden van vacaturefraude.

Om te bepalen welke mate van beveiliging noodzakelijk is, maakt UWV onder andere gebruik van het *BIV-classificatiedocument*. Naar mate de persoonsgegevens in een hogere vertrouwelijkheidsklasse vallen, worden strengere eisen gesteld aan de beveiligingsmaatregelen. In hoofdstuk 7 wordt meer in detail ingegaan op de beveiliging van persoonsgegevens en de wijze waarop UWV daar invulling aan geeft.

Voor de toepassing van dit beginsel zijn de volgende vragen steeds relevant:

- Is duidelijk onder welke vertrouwelijkheidsklasse de persoonsgegevens vallen die worden verwerkt?
- Zijn adequate technische en organisatorische maatregelen getroffen om de persoonsgegevens te beveiligen?

3.8. Privacybeginselen moeten al bij het ontwerpen en inrichten van processen en systemen een plaats krijgen (*security & privacy by design/default*)

Wat zegt de AVG?

Iedere organisatie die persoonsgegevens verwerkt moet ervoor zorgen dat de hierboven genoemde privacybeginselen bij het ontwerpen en inrichten van de processen en systemen worden meegenomen en dat passende technische en organisatorische maatregelen vanaf het begin worden getroffen. Dit wordt ook wel *privacy by design* en *privacy by default* genoemd.

Artikel 25 AVG

Privacy begint op de tekentafel. Dit betekent dat bij het ontwerpen of wijzigen van processen en bij het bouwen of laten bouwen van nieuwe systemen, steeds bovengenoemde beginselen moeten worden meegenomen. Dit wordt ook wel *privacy by design* en *privacy by default* genoemd. Het vanaf de start rekening houden met deze beginselen is van belang omdat het achteraf inbouwen van maatregelen meestal duurder en inefficiënt is. Ook bij een aanbesteding voor een project waarin sprake is van verwerking van persoonsgegevens moet dit een onderdeel vormen van de *requirements*.¹⁹ Procesontwerpers moeten daarom kennis hebben van deze beginselen zodat deze bij het ontwerp van processen worden meegenomen. Datzelfde geldt voor de personen die betrokken zijn bij het (laten) ontwerpen en bouwen van nieuwe systemen.

Het door CISO opgestelde beleidsstuk *Security & Privacy by design en by default* geeft nadere invulling hoe deze principes een plaats hebben in het voortbrengingsproces. En ook in het document Gegevensprincipes UWV (van Data Office), waarin richtinggevende uitspraken over de gegevenshuishouding worden gedaan, wordt bij het principe van *privacy by design* aangesloten. Daarnaast ondersteunt het instrument gegevensbeschermingseffectbeoordeling (GEB) bij het overdenken van de hierboven genoemde vragen. De GEB komt in paragraaf 11.1 aan de orde.

3.9. UWV beleidskader privacybeginselen

- **Alle organisatieonderdelen van UWV zorgen ervoor dat alle verwerkingen van persoonsgegevens voldoen aan de in dit hoofdstuk genoemde beginselen.**
- **Bij de verwerking van persoonsgegevens en bij het ontwerpen en inrichten van nieuwe processen en systemen worden daarom steeds in ieder geval de volgende vragen beantwoord:**
 - Is er een grondslag voor de verwerking?
 - Is voor degene van wie persoonsgegevens worden verwerkt duidelijk dat dit gebeurt en met welk doel?
 - Is het doel van de verwerking duidelijk omschreven?
 - Zijn de gegevens die worden verwerkt noodzakelijk voor dat doel of zijn er andere methoden om het doel te bereiken waarbij minder persoonsgegevens worden verwerkt?
 - Staat de verwerking van de gegevens in redelijke verhouding tot het doel waarvoor de gegevens zijn verzameld?
 - Worden niet méér gegevens verzameld dan nodig is voor dat doel?
 - Hoe wordt ervoor gezorgd dat de gegevens up-to-date blijven?
 - Is duidelijk in welke vertrouwelijkheidsklasse de gegevens vallen?

¹⁹ Overweging 78 AVG

- **Zijn adequate technische en organisatorische beveiligingsmaatregelen getroffen?**
 - **Is de vernietiging/archivering van de gegevens geregeld?**
 - **Is het autorisatiebeheer zodanig geregeld dat niet meer mensen toegang hebben tot de gegevens dan redelijkerwijs noodzakelijk voor het doel, mede gelet op de aard van de gegevens?**
- **De organisatieonderdelen zorgen ervoor dat sleutelfiguren zoals procesontwerpers, productontwikkelaars, business analisten, business consultants, business adviseurs en architecten over voldoende kennis van de privacybeginselen beschikken, zodat zij deze bij het ontwerpen en inrichten van processen en systemen betrekken.**

4. Grondslagen voor de verwerking van persoonsgegevens

Verwerkingen van persoonsgegevens zijn alleen rechtmatig als zij zijn terug te voeren op tenminste één van de zes grondslagen die de AVG noemt.²⁰ In de volgende paragrafen wordt ingegaan op die grondslagen en op de vraag in welke gevallen UWV van die grondslagen gebruik kan maken.

Over het algemeen werkt UWV op basis van de grondslag zoals beschreven in paragraaf 4.1: de verwerking van persoonsgegevens is noodzakelijk voor uitvoering van een wettelijke taak van algemeen belang. Omdat de andere grondslagen wel kunnen voorkomen – UWV verwerkt immers gegevens in verschillende rollen – worden ze hier kort toegelicht. Raadpleeg Juridische Zaken indien de verwerking niet valt onder de grondslag ‘noodzakelijk ter uitvoering van onze wettelijke taken van algemeen belang’ of als er bij het bepalen van de grondslag voor een voorgenomen verwerking vragen zijn.

4.1. Noodzakelijk voor uitvoering van een wettelijke taak van algemeen belang

Wat zegt de AVG?

Persoonsgegevens mogen worden verwerkt als dit noodzakelijk is om uitvoering te geven aan een taak van algemeen belang (overheidstaak) onder de voorwaarde dat die taak van algemeen belang in de wet is verankerd.

Artikel 6 lid 1 (e) en lid 3 AVG

De belangrijkste grondslag voor de verwerking van persoonsgegevens door UWV is dat de verwerking ‘noodzakelijk is voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen’.²¹ Voorwaarde is dat die taken in de wet zijn benoemd. De wetgever bepaalt namelijk welke taken aan de overheid worden opgedragen. Daarom noemen we deze grondslag ‘noodzakelijk ter uitvoering van een *wettelijke* taak van algemeen belang’. In dit verband wordt ook wel gesproken van de ‘publieke taak’ van UWV.

UWV heeft als zelfstandig bestuursorgaan de opdracht om een aantal taken van algemeen belang uit te voeren. Deze taken komen voort uit wetgeving, zoals de Wet SUWI²² en verschillende materiewetten, zoals de Werkloosheidswet, de Ziektewet, de WIA en Wajong-wetgeving. In samenhang met artikel 6 lid 1 sub (e) AVG, voorzien deze wetten UWV van een grondslag om voor die taken noodzakelijke persoonsgegevens te verzamelen, te gebruiken en zo nodig aan (keten)partners te verstrekken (altijd met inachtneming van alle privacybeginselen zoals toegelicht in hoofdstuk 4). Het gaat hierbij bijvoorbeeld om de taken in verband met de rechtmatige verstrekking van uitkeringen (dus ook handhaving), dienstverlening in het kader van re-integratie en arbeidsbemiddeling, het uitvoeren van sociaal-medische beoordelingen en het vaststellen van het arbeidsvermogen. Ook vallen hieronder de taken van UWV in verband met het beheer van de polisadministratie en de verstrekking van gegevens daaruit aan daartoe gerechtigde afnemers. De verwerking van persoonsgegevens in verband met deze taken is op bovengenoemde grondslag gestoeld.

Van belang is nog te noemen dat de verwerking van persoonsgegevens in dit kader zich dient te beperken tot die persoonsgegevens die *noodzakelijk* zijn voor uitvoering van de genoemde taken. Zie ook het in paragraaf 3.4 genoemde beginsel van data-minimalisatie en proportionaliteit. Als méér persoonsgegevens worden verwerkt

²⁰ Artikel 6 lid 1 AVG.

²¹ Uitoefening van openbaar gezag betekent dat de organisatie bevoegd is om eenzijdig beslissingen te nemen die de rechtspositie van personen verandert/raakt. UWV oefent ook openbaar gezag uit omdat UWV bijvoorbeeld eenzijdig beslist over het al dan niet toekennen van een uitkering aan een burger.

²² Zie bijvoorbeeld de artikelen 30 e.v. Wet SUWI.

dan noodzakelijk is voor de uitvoering van deze taken en een andere grondslag daarvoor ontbreekt, dan is de verwerking van die gegevens onrechtmatig.

Het bovenstaande betekent dat bij nieuwe (samenwerkings)initiatieven altijd moet worden vastgesteld dat de wet of andere regelgeving (bijv. een AmvB) een basis biedt voor de verwerking (waaronder ook de verstrekking valt) van de persoonsgegevens. UWV is geregeld partij bij een convenant waarin afspraken voor samenwerking worden gemaakt. Een dergelijk convenant vormt echter geen grondslag voor de verwerking en het delen van persoonsgegevens. Uitgangspunt is dat de grondslag hiervoor in een wet of andere regelgeving moet zijn terug te vinden.²³ Als hierover twijfel bestaat dan moet Juridische Zaken worden geconsulteerd.

4.2. Noodzakelijk voor de uitvoering van een overeenkomst

Wat zegt de AVG?

Persoonsgegevens mogen worden verwerkt indien die verwerking noodzakelijk is voor de uitvoering van een overeenkomst met de betrokkene of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen.

Artikel 6 lid 1 (b) AVG

UWV sluit met verschillende personen overeenkomsten waarbij de verwerking van persoonsgegevens van de persoon waarmee de overeenkomst wordt gesloten noodzakelijk kan zijn ter uitvoering van die overeenkomst. Het gaat bijvoorbeeld om een arbeidsovereenkomst met nieuwe medewerkers, de inhuur van externen of het contract met een jobcoach. In dit laatste geval moet onderscheid worden gemaakt tussen de gegevens van de klant (die verwerkt worden op de grondslag wettelijke taak van algemeen belang, zoals beschreven in 4.1) en de gegevens van de jobcoach zelf, zoals een persoonlijk telefoonnummer. Alleen deze laatste kan UWV in deze context op basis van de grondslag 'uitvoering van een overeenkomst' verwerken. Op basis van deze grondslag mogen alleen de persoonsgegevens van de persoon waarmee de overeenkomst wordt gesloten worden verwerkt die noodzakelijk zijn voor de uitvoering van de overeenkomst – aanvullende persoonsgegevens mogen niet worden verwerkt. Voor dit laatste aspect zou mogelijk de grondslag gerechtvaardigd belang kunnen dienen (paragraaf 4.4) en in uitzonderlijke gevallen toestemming van de betrokkene (paragraaf 4.6).

Soms bestaat het misverstand dat de grondslag 'noodzakelijk voor de uitvoering van een overeenkomst' kan worden gebruikt om gegevens van bijvoorbeeld klanten te verstrekken aan een organisatie waarmee UWV een overeenkomst heeft gesloten. Denk hierbij bijvoorbeeld een onderzoeksbureau dat in opdracht van UWV een klantonderzoek verricht. Of een re-integratiebureau waarmee UWV een overeenkomst heeft gesloten voor het verlenen van re-integratiediensten aan onze klanten. De grondslag 'noodzakelijk ter uitvoering van een overeenkomst' is echter uitsluitend bedoeld om persoonsgegevens van degene waarmee de overeenkomst wordt gesloten te verwerken. Deze grondslag kan daarom nooit worden gebruikt om klantgegevens aan een partij waarmee de overeenkomst wordt gesloten te verstrekken. De klanten zijn immers geen partij bij de overeenkomst.

UWV sluit met ketenpartners of met andere publieke of private partijen regelmatig convenanten. Ook een dergelijk convenant is feitelijk een overeenkomst zoals hierboven genoemd. Ook voor convenanten geldt dat zij geen grondslag zoals bedoeld in deze paragraaf kunnen vormen voor de verwerking van gegevens van de klant.

²³ In uitzonderlijke gevallen kan – in overleg met JZ – toestemming van de betrokkene als grondslag dienen.

4.3. Noodzakelijk om te voldoen aan een wettelijke verplichting

Wat zegt de AVG?

Persoonsgegevens mogen worden verwerkt als dit noodzakelijk is om aan een wettelijke verplichting te voldoen.

Artikel 6 lid 1 (c) AVG

Een derde grondslag die de AVG noemt voor de rechtmatige verwerking van persoonsgegevens is dat de verwerking van de gegevens noodzakelijk is om te voldoen aan een wettelijke verplichting. Het gaat hierbij om situaties waarin de wet organisaties *verplicht* bepaalde persoonsgegevens te verwerken. Deze grondslag is daarom echt anders dan de in paragraaf 4.1 beschreven grondslag (noodzakelijk ter uitvoering van een wettelijke taak van algemeen belang).²⁴

Een aantal wetten verplicht organisaties om bepaalde persoonsgegevens vast te leggen, te verstrekken of te bewaren. Hierbij kan je denken aan de belastingwetgeving die de werkgever verplicht om bepaalde gegevens van de werknemer te registreren. Ook kan een organisatie op basis van het Wetboek van Strafvordering verplicht zijn om bepaalde gegevens aan de officier van justitie te verstrekken die hij nodig heeft voor een opsporingsonderzoek.

Ook op UWV rusten dergelijke wettelijke verplichtingen. Daarom kan deze grondslag ook de basis vormen voor de verwerking van persoonsgegevens door UWV. Voor UWV gaat het hierbij bijvoorbeeld om:

- Verplichtingen op grond van fiscaal recht of arbeidsrecht (bijv. de verplichting van een werkgever om een kopie van het identiteitsbewijs van de werknemer in de salarisadministratie op te nemen);
- Verplichtingen tot het verstrekken van persoonsgegevens op basis van de Algemene wet bestuursrecht (Awb);
- Verplichtingen in verband met strafrechtelijke handhaving of nationale veiligheid bijv. op basis van het Wetboek van Strafvordering.

4.4. Noodzakelijk ter behartiging van een gerechtvaardigd belang

Wat zegt de AVG?

Persoonsgegevens mogen worden verwerkt indien dit noodzakelijk is voor de behartiging van een gerechtvaardigd belang van de verwerkingsverantwoordelijke of een derde, mits de belangen van de betrokkene niet zwaarder wegen dan dat gerechtvaardigde belang. Overheidsorganisatie mogen hun wettelijke taken niet zelfstandig 'uitbreiden' door op deze grondslag persoonsgegevens te verwerken die noodzakelijk zijn voor de uitvoering van een publieke taak. Maar zij mogen deze grondslag wel gebruiken voor verwerkingen die noodzakelijk zijn in het kader van een veilige en efficiënte bedrijfsvoering, zoals bijvoorbeeld het loggen en monitoren van de toegang van medewerkers tot de systemen.

Artikel 6 lid 1 (f) AVG

Uitgangspunt is dat de verwerking van persoonsgegevens door overheidsinstanties bij de uitvoering van hun publieke taken altijd moet zijn gebaseerd op een wettelijke bepaling. Alleen de wetgever bepaalt welke taken UWV heeft waarvoor het persoonsgegevens mag verwerken. Daarom mogen overheidsorganisaties geen gebruik maken van de grondslag 'gerechtvaardigd belang' om daarmee hun publieke taken (het primaire proces) uit te breiden.

UWV mag deze grondslag wel gebruiken voor verwerkingen in ondersteunende processen, wanneer het gaat om verwerking van persoonsgegevens in het kader van een veilige en efficiënte bedrijfsvoering. Het gaat dan in veel gevallen om verwerking van gegevens van medewerkers. Zo is de verwerking van persoonsgegevens door

²⁴ De verwerkingen van persoonsgegevens van UWV die noodzakelijk zijn om uitvoering te geven aan de Wet SUWI en andere sociale zekerheidswetten vinden hun grondslag in 'noodzakelijk ter uitvoering van een wettelijke taak van algemeen belang'.

Bureau Integriteit op deze grondslag gestoeld. Maar ook camerabewaking en bezoekersregistratie waarbij gegevens van klanten worden verwerkt is op deze grondslag gestoeld. Ook in de contractuele relatie met partners kan deze grondslag gebruikt worden. Voorbeelden hiervan zijn het verstrekken van gegevens van een medewerker aan een bloemist om een bloemetje te sturen aan een collega.

Wanneer UWV van deze grondslag gebruik wil maken, zal steeds een belangenafweging moeten worden gemaakt tussen het gerechtvaardigd belang dat UWV wenst te behartigen (de reden waarom UWV persoonsgegevens wil verwerken) en de belangen van de betrokkene (medewerkers, bezoekers) van wie persoonsgegevens in dat verband worden verwerkt. De Autoriteit Persoonsgegevens heeft de voorwaarden voor deze belangenafweging opgesomd.²⁵ Als UWV gebruik wil maken van de grondslag gerechtvaardigd belang, zullen de volgende stappen moeten worden doorlopen en worden vastgelegd (bijvoorbeeld in een GEB):

1. Beschrijf wat het gerechtvaardigd belang is.
2. Motiveer waarom de (voorgenomen) verwerking noodzakelijk is om dit belang te behartigen. Schenk hierbij aandacht aan de beginselen van *proportionaliteit* (staat het doel van de verwerking in redelijke verhouding staat tot de inbreuk op de privacy van de betrokkenen) en *subsidiariteit* (kan het doel niet op een andere, voor de betrokkene minder ingrijpende manier worden bereikt).
3. Beschrijf de afweging die is gemaakt tussen de belangen van UWV en die van de betrokkenen. Betrek daarbij:
 - a. de gevolgen van de verwerking voor de betrokkenen;
 - b. hoe ernstig de inbreuk is op de privacy van de betrokkenen;
 - c. welke (aanvullende) maatregelen zijn genomen om ongewenste gevolgen voor de betrokkenen te voorkomen of beperken;
 - d. of de betrokkenen de verwerking min of meer kunnen verwachten, bijvoorbeeld als vervolg op een eerdere verwerking die noodzakelijk was om een contract uit te voeren.

In zijn algemeen kan worden gesteld dat hoe gevoeliger de persoonsgegevens zijn, hoe zwaarder het gerechtvaardigd belang zal moeten zijn. Omdat dit een lastige afweging betreft, moet altijd Juridische Zaken worden geraadpleegd wanneer deze grondslag wordt overwogen. Uiteindelijk zal degene die verantwoordelijk is voor de voorgenomen verwerking met inachtneming van het advies van Juridische Zaken de belangenafweging maken. Voor de volledigheid wordt nog opgemerkt dat bepaalde verwerkingen van persoonsgegevens van medewerkers van UWV die op deze grondslag kunnen zijn gestoeld (bijvoorbeeld monitoring en surveillance van medewerkers) ook de instemming van de Ondernemingsraad behoeven.

4.5. Noodzakelijk ter bescherming van een vitaal belang

Wat zegt de AVG?

Persoonsgegevens kunnen worden verwerkt wanneer dit – kort gezegd – noodzakelijk is in verband met vitale belangen van de betrokkene of een derde. Het gaat hier om situaties van leven of dood waarin het niet mogelijk is om de betrokkene om toestemming te vragen.

Artikel 6 lid 1 (d) AVG

Deze grondslag is voor de *dienstverlening* van UWV niet relevant. Deze grondslag heeft namelijk betrekking op de situatie dat de verwerking van persoonsgegevens noodzakelijk is in verband met de acute gezondheidstoestand van de betrokkene of een derde. Het gaat hier om situaties van leven en dood waarin de betrokkene, bijvoorbeeld omdat deze bewusteloos is, zelf geen toestemming kan geven. Deze situaties doen zich in de regel niet voor bij de uitvoering van de taken van UWV.

De grondslag zou mogelijk wel aan de orde kunnen zijn wanneer een medewerker of bezoeker van UWV onwel is geworden en relevante gegevens over de betrokkene, bijvoorbeeld door een BHV'er, aan het ambulancepersoneel moeten worden verstrekt.

²⁵ <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/mag-u-persoonsgegevens-verwerken#hoe-toetst-u-of-u-zich-mag-baseren-op-de-grondslag-gerechtvaardigd-belang-7531>

4.6. Verwerking op basis van toestemming van de betrokkene

Wat zegt de AVG?

Persoonsgegevens mogen worden verwerkt indien de betrokkene daarvoor vooraf – geïnformeerd en in volledige vrijheid – ondubbelzinnig toestemming heeft gegeven. Die toestemming kan op ieder moment worden ingetrokken. Dit heeft tot gevolg dat de verwerking op basis van toestemming moet worden gestaakt. *Artikel 6 lid 1 (a) en artikel 7 AVG*

Indien een organisatie zich niet kan beroepen op één van de voorgaande vijf grondslagen, dan blijft alleen toestemming van de betrokkene over als grondslag om persoonsgegevens te verwerken. Voor UWV is toestemming, wanneer het om onze klanten gaat, in principe geen geldige grondslag. Dit heeft te maken met de strenge eisen die aan toestemming worden gesteld. Een belangrijke eis is namelijk dat de toestemming *in volledige vrijheid* moet zijn gegeven. Onze klanten bevinden zich ten opzichte van UWV in een ongelijkwaardige positie. Zij zijn immers van UWV afhankelijk voor de verstrekking van hun uitkering en het beeld kan bestaan dat weigeren toestemming te geven nadelige gevolgen voor de klanten zou hebben. Dit maakt het onwaarschijnlijk dat zij volledig vrij zijn, om al dan niet toestemming te verlenen. Dit geldt overigens in beginsel voor alle overheidsorganisaties.²⁶ Daarom maakt UWV in beginsel géén gebruik van toestemming als grondslag voor de verwerking van persoonsgegevens van onze klanten. Alleen in zeer uitzonderlijke gevallen kan – in overleg met Juridische Zaken – van dit uitgangspunt worden afgeweken.

Ook tussen werkgever en werknemer bestaat een afhankelijkheidsrelatie. Een werknemer zal zich niet altijd vrij voelen om toestemming te weigeren wanneer hij het idee kan hebben dat dit gevolgen heeft voor zijn positie. Daarom geldt dat werkgevers zeer terughoudend moeten zijn wanneer zij persoonsgegevens van werknemers op deze grondslag willen verwerken. Voor UWV geldt daarom als uitgangspunt dat in beginsel geen gegevens van medewerkers op basis van toestemming worden verwerkt. Uitzondering hierop is mogelijk in incidentele gevallen waarin volstrekt duidelijk is dat het al dan niet toestemming verlenen geen gevolgen heeft voor het dienstverband van de medewerker. Denk bijvoorbeeld aan de registratie van persoonsgegevens voor de sportdag, het gebruik van foto's van medewerkers voor intern gebruik en social media-uitingen van UWV (beeldbank) of de verwerking van gegevens in het kader van een medewerkersenquête.

Toestemming als grondslag voor de structurele verwerking van persoonsgegevens is bovendien onwenselijk omdat de toestemming op ieder moment door de betrokkene kan worden ingetrokken (hij of zij dient ook op die mogelijkheid te worden gewezen), waardoor de verwerking van persoonsgegevens direct moet worden gestaakt. Nog los van wat dit betekent voor de dienstverlening is dit ook administratief gezien problematisch.

Het vragen om toestemming 'voor de zekerheid' in situaties waar dit niet wettelijk is voorgeschreven en ook niet noodzakelijk is (omdat er al een andere grondslag bestaat), moet vermeden worden. Het suggereert namelijk dat de betrokkene de mogelijkheid heeft om betekenisvol zijn toestemming in te trekken, terwijl die intrekking geen gevolgen zal hebben voor de voortgang van de verwerking van de gegevens. Deze vindt immers al op een andere grondslag plaats. Vraag dus niet 'voor de zekerheid' om toestemming en maak duidelijk waarom UWV bevoegd is de persoonsgegevens te verwerken.

Gebruik van cookies en andere technieken om gegevens van websitebezoekers te verwerken

Toestemming als grondslag voor gegevensverwerking moet niet verward worden met toestemming voor het gebruik van cookies. Cookies die noodzakelijk zijn om de functionaliteit van de website te verzorgen kunnen zonder toestemming geplaatst worden. Ditzelfde geldt voor cookies die de kwaliteit of effectiviteit van de website meten, maar alleen voor zover deze geen of minimale inbreuk op de privacy van de bezoeker maken. Wel moet er nog altijd een grondslag onder de AVG zijn om deze persoonsgegevens te verwerken.

Indien cookies of andere tracking-devices die het digitale (klant)gedrag vastleggen worden gebruikt en deze meer dan een minimale inbreuk op de privacy van de bezoeker maken, moet aan de betrokkene toestemming worden gevraagd. Deze toestemming is vereist op grond van de Telecommunicatiewet. Pas als er toestemming is gegeven, mogen dergelijke cookies en trackingtools worden geplaatst.

²⁶ Zie ook Overweging 43 AVG.

Toestemming in het kader van het verwerken van gegevens die vallen onder het medisch beroepsgeheim

Bij SMZ wordt in een aantal situaties gebruik gemaakt van toestemming van de klant om bepaalde gegevens op te vragen bij een behandelend arts of om gegevens te delen met een advocaat of medisch adviseur. In deze situaties betreft de gevraagde toestemming van de klant de toestemming om het medisch beroepsgeheim te doorbreken zodat de gegevens kunnen worden gedeeld.²⁷ De verdere verwerking van de gegevens bij UWV gebeurt echter niet op basis van de AVG grondslag toestemming, maar op basis van de grondslag 'noodzakelijk voor een wettelijke taak van algemeen belang' omdat de gegevens worden verwerkt om de publieke taak van UWV uit te voeren.

4.7. UWV beleidskader grondslagen

- De belangrijkste grondslag voor de verwerking van persoonsgegevens door UWV is dat de verwerking noodzakelijk is voor de uitvoering van een taak van algemeen belang. Als dit de grondslag vormt van de verwerking moet er altijd een specifieke wettelijke bepaling - bijvoorbeeld in de Wet SUWI of een andere een sociale zekerheidswet - kunnen worden aangewezen waarin die taken aan UWV worden opgedragen.
- Als een voorgenomen verwerking gestoeld wordt op een andere grondslag dan 'noodzakelijk ter uitvoering van een wettelijke taak van algemeen belang', wordt Juridische zaken geraadpleegd om de geldigheid van de grondslag te toetsen.
- Andere grondslagen op basis waarvan UWV persoonsgegevens kan verwerken betreffen:
 - de verwerking is noodzakelijk voor het afsluiten of uitvoeren van een overeenkomst (het kan dan alleen gaan om de persoonsgegevens van degene waarmee de overeenkomst wordt afgesloten); of
 - de verwerking is noodzakelijk om aan een wettelijke verplichting te voldoen (bijvoorbeeld de verplichting voor UWV om een kopie van het identiteitsbewijs van de werknemer in de salarisadministratie op te nemen).
- UWV kan de verwerking van persoonsgegevens ook baseren op de grondslag van behartiging van een gerechtvaardigd belang, doch uitsluitend wanneer UWV optreedt als werkgever of contractspartner. Dus niet in het kader van de uitvoering van publieke taken.
- Voor UWV is toestemming, wanneer het om de klanten van UWV gaat, in principe geen geldige grondslag voor verwerking van gegevens. In uitzonderlijke gevallen kan hiervan worden afgeweken na overleg met JZ en de FG.
- De grondslag van voorgenomen verwerkingen moet worden onderbouwd en vastgesteld voordat de verwerking wordt uitgevoerd. De grondslag wordt in een GEB en in het register van verwerkingen vastgelegd.

²⁷ Artikel 88 Wet BIG en artikel 7:457 lid 1 BW

5. Verwerkingen van persoonsgegevens bij UWV

In dit hoofdstuk wordt nader ingegaan op de verwerking van persoonsgegevens bij UWV. Zoals in hoofdstuk 2 is toegelicht, zijn persoonsgegevens alle gegevens met betrekking tot een persoon waarvan de identiteit al bekend is of een nog onbekende persoon die aan de hand van die gegevens kan worden geïdentificeerd. Een verwerking in de zin van de AVG betreft iedere bewerking van persoonsgegevens of van een geheel van persoonsgegevens (zoals een database met persoonsgegevens). Hieruit volgt dat vrijwel alles dat UWV met persoonsgegevens doet als een verwerking in de zin van de AVG moet worden opgevat. In dit hoofdstuk wordt een aantal van deze verwerkingen nader toegelicht.

Het hoofdstuk start met een toelichting op de verwerking van extra gevoelige persoonsgegevens, zoals bijzondere persoonsgegevens (paragraaf 5.1), persoonsgegevens van strafrechtelijke aard (paragraaf 5.2) en het burgerservicenummer (BSN). Vervolgens wordt in de paragrafen 5.4 t/m 5.9 een aantal andere specifieke aspecten van de verwerking van persoonsgegevens bij UWV besproken.

5.1. Bijzondere persoonsgegevens

Wat zegt de AVG?

Bijzondere persoonsgegevens zijn persoonsgegevens over ras, gezondheid, politieke en religieuze opvattingen, seksuele voorkeur, vakbondslidmaatschap, genetische en biometrische gegevens. De AVG kent als uitgangspunt een verbod om bijzondere persoonsgegevens te verwerken. Alleen indien sprake is van één van de in de AVG en UAVG genoemde uitzonderingen, mogen bijzondere persoonsgegevens worden verwerkt. *Artikel 9 AVG, artikelen 22 t/m 30 UAVG*

De volgende gegevens zijn in de AVG als bijzondere persoonsgegevens aangemerkt:

- gegevens waaruit ras of etnische afkomst blijkt (hieronder kunnen onder omstandigheden ook foto's en camerabeelden van personen vallen, zie ook paragraaf 6.1.2);
- gegevens waaruit het lidmaatschap van een vakbond blijkt;
- gegevens waaruit politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen blijken;
- genetische gegevens (bijv. een DNA-profiel);
- biometrische gegevens, maar alleen wanneer deze ten behoeve van de unieke identificatie van een persoon worden verwerkt (bijv. een pasfoto, vingerafdruk of irisscan die wordt gebruikt om iemand toegang tot een gebouw of ruimte te verlenen);
- gegevens over de lichamelijke of geestelijke gezondheid van een persoon (zie paragraaf 5.1.1);
- gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.

Bijzondere persoonsgegevens zijn gevoelig van aard omdat mensen op grond van deze gegevens gemakkelijk kunnen worden gestigmatiseerd of gediscrimineerd. De informatie die bijzondere persoonsgegevens over iemand prijsgeeft kan eenvoudig tegen die persoon worden gebruikt. Daarom mogen bijzondere persoonsgegevens in beginsel niet worden verwerkt. Alleen als zich een in de AVG en UAVG genoemde uitzondering voordoet, mogen bijzondere persoonsgegevens worden verwerkt. Uiteraard dient eerst de voorliggende vraag te worden beantwoord of er überhaupt een grondslag voor de verwerking is (zie hoofdstuk 4).

Ook voor UWV geldt het algemene verbod dat bijzondere persoonsgegevens niet mogen worden verwerkt. Voor sommige bijzondere persoonsgegevens, zoals bijvoorbeeld voor gezondheidsgegevens, geldt echter een uitzondering op grond waarvan UWV wel bepaalde bijzondere persoonsgegevens mag verwerken. Deze uitzonderingen worden in de volgende paragrafen doorgenomen.

Wat zeggen de AVG en de UAVG?

De AVG en UAVG kennen een aantal uitzonderingen op het algemene verbod om gezondheidsgegevens te verwerken. Ook voor UWV geldt zo'n uitzondering. UWV mag gezondheidsgegevens verwerken – kort gezegd - voor zover dit noodzakelijk is voor de uitvoering van zijn taken op het gebied van sociale zekerheid in verband met arbeidsgeschiktheid en voor de re-integratie en arbeidsbemiddeling, voor zover deze taken in nationale wetgeving zijn verankerd.

Artikel 9 lid 2 (b) en (h) van de AVG en artikel 30 van de UAVG

Gezondheidsgegevens: een ruim begrip

Gezondheidsgegevens zijn persoonsgegevens die verband houden met de lichamelijke of geestelijke gezondheid van een persoon. In eerste instantie wordt hierbij gedacht aan een medische rapportage waarin bijvoorbeeld de diagnoses en behandeling van een patiënt wordt beschreven. Maar het begrip gezondheidsgegevens is aanzienlijk ruimer. Onder dit begrip vallen ook gegevens over verleende gezondheidszorgdiensten waarmee informatie over de gezondheidstoestand van die persoon wordt gegeven²⁸. Hierbij kan je denken aan het feit dat een persoon een afspraak heeft met een arts of verloskundige. Ook die informatie geeft al iets prijs over de gezondheidstoestand van de betrokkene. Maar ook het enkele feit dat een persoon een WIA-uitkering heeft of een ziekmelding van een zieke medewerker, is een gezondheidsgegeven.

Gezondheidsgegevens is kortom een ruim begrip waaronder alle gegevens vallen die verband houden met de lichamelijke of geestelijke gezondheid van een persoon.

Uitzondering op verbod van verwerking van gezondheidsgegevens

Omdat gezondheidsgegevens bijzondere persoonsgegevens zijn, mogen ze alleen onder strikte voorwaarden worden verwerkt. Voor de taken van UWV is in de wet een uitzondering gemaakt op het verbod om gezondheidsgegevens te verwerken. Gezondheidsgegevens mogen door bestuursorganen (zoals UWV), pensioenfondsen, werkgevers of instellingen die voor hen werkzaam zijn (zoals bijvoorbeeld een arbo-dienst, maar ook een leverancier die in opdracht van UWV optreedt) worden verwerkt, maar alleen voor zover dat noodzakelijk is voor:

- a) een goede uitvoering van wettelijke voorschriften, pensioenregelingen of cao's die voorzien in het recht op een uitkering of andere aanspraken die afhankelijk zijn van de gezondheidstoestand van de betrokkene;
- b) de re-integratie of begeleiding van werknemers en uitkeringsgerechtigden in verband met ziekte of arbeidsongeschiktheid.

De AVG eist daarnaast dat personen die voor deze doeleinden gezondheidsgegevens verwerken, gebonden zijn aan een geheimhoudingsplicht.²⁹ Omdat op grond van artikel 74 van de Wet SUWI voor alle medewerkers van UWV sowieso een geheimhoudingsplicht geldt, wordt aan deze verplichting van de AVG voldaan.

Het feit dat UWV gebruik kan maken van een uitzondering op het verbod om gezondheidsgegevens te verwerken is in zichzelf nog niet voldoende. Er moet daarnaast ook sprake zijn van een grondslag voor de verwerking (zie ook hoofdstuk 4).

Het voorgaande betekent dat op grond van de AVG en de UAVG medewerkers van UWV, in het bijzonder bij de divisies SMZ, WERKbedrijf³⁰, Uitkeren en Bezwaar en Beroep, gezondheidsgegevens mogen verwerken als dit noodzakelijk is voor de uitvoering van hun wettelijke taken. Omdat het hier om bijzondere persoonsgegevens gaat, moet hierbij extra zorgvuldig worden gekeken naar de beginselen van doelbinding en proportionaliteit en naar passende beveiligingsmaatregelen om de vertrouwelijkheid van de gegevens te beschermen. (zie ook de *UWV Richtlijn Omgaan met Gezondheidsgegevens*, voorheen: *Richtlijn beheer gegevens vallend onder het medisch beroepsgeheim van de verzekeringsarts*)

²⁸ Artikel 4 lid 15 AVG

²⁹ Artikel 9 lid 3 AVG.

³⁰ Inclusief de arbeidsjuridische dienstverlening.

Hoewel medewerkers van UWV bevoegd zijn om gezondheidsgegevens te verwerken indien dit noodzakelijk is voor de wettelijke taken, zijn sommige taken voorbehouden aan de verzekeringsarts. Die taken mogen dus alleen door een verzekeringsarts worden verricht of door een medewerker van UWV onder verantwoordelijkheid van de verzekeringsarts. De Autoriteit Persoonsgegevens heeft UWV erop gewezen dat waar werkzaamheden zijn voorbehouden aan een verzekeringsarts, zoals het geven van een sociaal medisch oordeel in verband met het al dan niet toekennen van het recht op een uitkering, deze werkzaamheden niet zelfstandig door een 'gewone' medewerker kunnen worden verricht.³¹ Zie hiervoor ook de *UWV Richtlijn Omgaan met Gezondheidsgegevens*.

Gezondheidsgegevens en vertrouwelijkheidsklasse

Zoals in het begin van deze paragraaf is toegelicht, kent de AVG een ruime definitie van het begrip gezondheidsgegevens, variërend van 'een afspraak met een arts' tot een diagnoserapport van een specialist. UWV verwerkt op grote schaal gezondheidsgegevens om zijn wettelijke taken uit te kunnen voeren en heeft daarbij te maken met gegevens uit het hele spectrum van deze definitie. Al deze gezondheidsgegevens betreffen bijzondere persoonsgegevens onder de AVG, waarvan de vertrouwelijkheid goed moet worden beschermd. UWV heeft er voor gekozen om binnen deze groep gezondheidsgegevens een groep van extra gevoelige gegevens te onderscheiden die extra bescherming genieten. Dit zijn de gezondheidsgegevens die in vertrouwelijkheidsklasse 3 van de BIV-classificatie vallen. Het gaat hierbij om gezondheidsgegevens zoals de diagnose van een arts of de uitslag van een bloedonderzoek. Deze gezondheidsgegevens wil UWV nog beter beschermen dan meer administratieve gezondheidsgegevens zoals het feit dat iemand een WIA-uitkering heeft of dat iemand een afspraak heeft met een verloskundige. In het kader van deze extra gevoelige gezondheidsgegevens wordt in de uitvoeringspraktijk ook wel over 'medische gegevens' gesproken. Deze terminologie komt echter niet voor in de AVG.

Het onderscheid binnen gezondheidsgegevens maakt UWV alleen in het kader van gegevensbescherming; voor alle gezondheidsgegevens geldt dat deze bijzondere persoonsgegevens onder de AVG betreffen en dat deze uitsluitend op basis van een van de uitzonderingsgronden door UWV mogen worden verwerkt. (zie ook hoofdstuk 7 van dit beleidskader en het *UWV BIV classificatiedocument 2.0*)

Medisch beroepsgeheim

Gezondheidsgegevens, waaronder de groep gezondheidsgegevens die UWV heeft aangewezen als extra gevoelige gegevens in vertrouwelijkheidsklasse 3, moeten niet verward worden met gegevens die vallen onder het medisch beroepsgeheim. Het medisch beroepsgeheim verbiedt artsen in beginsel gegevens te delen die hen uit hoofde van hun beroep door een patiënt zijn toevertrouwd, tenzij de betrokkene uitdrukkelijk toestemming heeft gegeven voor de betreffende gegevensdeling.³² Het medisch beroepsgeheim beperkt zich echter niet tot gezondheidsgegevens, maar betreft alle soorten gegevens die de patiënt met de arts deelt. Het gaat daarbij dus niet per definitie om bijzondere persoonsgegevens. Niet het *type* gegevens is doorslaggevend, maar *de situatie*, namelijk dat de gegevens met de arts zijn gedeeld.

Ook op de verzekeringsartsen van UWV rust het medisch beroepsgeheim, zij het in aangepaste vorm. De verzekeringsarts werkt immers niet in opdracht van de patiënt, maar in opdracht van een derde, namelijk het UWV. Hierdoor mag een verzekeringsarts bepaalde gegevens die onder het medisch beroepsgeheim vallen toch delen, maar alleen voor zover hij daartoe op grond van de wet bevoegd of verplicht is.³³ Op grond van artikel 74 lid 4 Wet SUWI is hij bevoegd gezondheidsgegevens die onder het medisch beroepsgeheim vallen te delen met medewerkers van UWV, voor zover dit:

- noodzakelijk is voor de uitoefening van hun taken;
- die taken vallen binnen de hierboven omschreven uitzonderingen onder a) en b); en
- niet méér gegevens worden verstrekt dan strikt noodzakelijk zijn voor die taken.

Voor de verwerking van persoonsgegevens in de situatie dat deze aan een arts zijn toevertrouwd gelden dus naast de vereisten van de (U)AVG ook het medisch beroepsgeheim. Bovendien kennen artsen een eigen wettelijk kader met de Wet op de beroepen in de individuele gezondheidszorg (Wet BIG) en de Wet op de geneeskundige behandelovereenkomst (WGBO). Het strekt te ver om hier in dit UWV beleidskader privacy

³¹ Onderzoeksrapport Autoriteit persoonsgegevens over het verwerken van gezondheidsgegevens door medewerkers verzuimbeheersing van UWV.

³² Artikel 88 Wet BIG en artikel 7:457 lid 1 BW.

³³ Zie de richtlijnen van de KNMG, Omgaan met medische gegevens, p. 22 en 111. <https://www.knmg.nl/advies-richtlijnen/knmg-publicaties/omgaan-met-medische-gegevens.htm>

verder op in te gaan. Een nadere uitwerking van hoe om te gaan met gezondheidsgegevens binnen de praktijk van UWV is beschreven in de *UWV Richtlijn Omgaan met Gezondheidsgegevens* (voorheen: *Richtlijn beheer gegevens vallend onder het medisch beroepsgeheim van de verzekeringsarts*), zoals opgesteld door het Centraal Expertise Centrum (CEC) van UWV, en de *Regeling beheer en verkeer medische gegevens B&B*.

Verstrekking van gezondheidsgegevens intern binnen UWV en met externe partijen

Zoals gezegd mag UWV uitsluitend gezondheidsgegevens verwerken die noodzakelijk zijn voor de uitvoering van de hierboven onder a. en b. genoemde taken. Vanwege de gevoelige aard van de gegevens, mogen de noodzakelijke gezondheidsgegevens alleen worden gedeeld indien verzekerd is dat niet méér personen kennis nemen van die gegevens dan strikt noodzakelijk is voor de uitvoering van de desbetreffende taken.

Voorbeelden van onnodige verstrekking van gezondheidsgegevens zijn de volgende. Wanneer de bedrijfsarts contact heeft met Facilitair bedrijf in verband met het regelen van een tijdelijke parkeerplaats voor een medewerker is het onnodig om hierbij aan Facilitair Bedrijf meer informatie te verstrekken, zoals dat het gaat om een gebroken been. Dergelijke informatie heeft Facilitair Bedrijf niet nodig voor zijn taken en dient dus achterwege te blijven. Ook het verstrekken van gedetailleerde gezondheidsgegevens aan FEZ voor de betaling van een factuur is niet noodzakelijk en dient achterwege te blijven.

5.1.2. Foto's van personen, kopie van een identiteitsbewijs en camerabeelden

Een foto van een persoon (hieronder valt ook een kopie van een officieel identiteitsbewijs waarop een foto van de betrokkene staat) of camerabeelden waarop personen herkenbaar in beeld zijn gebracht, zijn persoonsgegevens. De verwerking hiervan moet dus voldoen aan alle eisen van de AVG (zie o.a. hoofdstuk 4 en 5). In bepaalde gevallen, maar zeker niet in alle gevallen, moeten foto's en camerabeelden als *bijzondere* persoonsgegevens worden aangemerkt. Om te bepalen of sprake is van verwerking van bijzondere persoonsgegevens, is het van belang na te gaan in welke context de foto/camerabeelden worden verwerkt en met welk doel ze worden verwerkt.

Foto's en camerabeelden waarop mensen herkenbaar in beeld zijn gebracht, moeten in ieder geval worden gekwalificeerd als bijzondere persoonsgegevens in de volgende twee gevallen:

- a) De verwerking van de foto/camerabeelden is bedoeld om daaruit het ras of de etnische afkomst van de afgebeelde personen af te leiden of het risico bestaat dat de foto/camerabeelden voor dat doel worden gebruikt (en dus dat het risico op discriminatie bestaat).
- b) De foto wordt verwerkt met behulp van bepaalde technische middelen met als doel de unieke identificatie of authenticatie van de persoon mogelijk te maken (biometrische gezichtsherkenning). UWV maakt hiervan op dit moment geen gebruik.

Foto's van personen genomen tijdens een bedrijfsuitje of in de context van communicatiedoeleinden³⁴ en foto's die door de directie Handhaving worden gemaakt in het kader van de toezichtstaak, zullen meestal *niet* als bijzondere persoonsgegevens worden aangemerkt.

Maar de verwerking van foto's in de personeelsadministratie of op een CV, kunnen wel als verwerking van bijzondere persoonsgegevens worden aangemerkt omdat hier het risico bestaat dat een medewerker of sollicitant wordt beoordeeld op ras of etnische achtergrond.

Als een foto/camerabeelden – gelet op de context en doel van de verwerking – als een bijzonder persoonsgegeven moet worden aangemerkt, mogen deze alleen worden verwerkt als zich een van de uitzonderingsgronden voor doet. De volgende uitzonderingsgronden kunnen in de context van UWV relevant zijn:

- de verwerking is onvermijdelijk met het oog op de identificatie van de betrokkene (denk hierbij aan een foto op een toegangspas of opnamen van een beveiligingscamera);³⁵
- de betrokkene heeft uitdrukkelijk toestemming gegeven voor de verwerking;³⁶
- de betrokkene heeft de persoonsgegevens kennelijk zelf openbaar gemaakt. Onder openbaar maken wordt hier verstaan dat de gegevens voor een breed publiek toegankelijk zijn.³⁷

³⁴ Denk bijvoorbeeld aan het gebruik van foto's op banners of posters. Maar let hierbij op want ook het portretrecht kan aan de orde zijn. Raadpleeg zo nodig Juridische Zaken.

³⁵ Artikel 25 sub (a) UAVG.

³⁶ Artikel 22 lid 2 sub (a) UAVG.

³⁷ Artikel 22 lid 2 sub (d) UAVG.

Profielfoto's die medewerkers zelf vrijwillig op Vinder hebben geplaatst, vallen onder de uitzonderingsgrond dat de betrokkene deze zelf openbaar heeft gemaakt. Betrokkene weet immers dat alle UWV-ers er dan kennis van kunnen nemen. Hij of zij is ook niet verplicht om een foto van zichzelf op de Vinder te plaatsen.

Een foto op een CV is een bijzonder persoonsgegeven omdat in het kader van het zoeken naar werk het risico bestaat dat er een onderscheid wordt gemaakt naar etnische afkomst. Wanneer een klant de foto met CV zelf op werk.nl plaatst en het is voor hem volstrekt duidelijk dat dit betekent dat alle werkgevers die hiertoe toegang hebben, dat CV inclusief de foto kunnen inzien (en wellicht ook downloaden), dan kan dit eveneens worden verwerkt op de grond dat de betrokkene dit zelf in deze context van werk.nl openbaar heeft gemaakt. Wanneer een klant echter een CV met pasfoto alleen aan een medewerker van UWV stuurt en dus niet op werk.nl openbaar maakt, zal alvorens dit CV inclusief foto mag worden verstrekt aan een werkgever, de klant hiervoor uitdrukkelijk (schriftelijk) toestemming moeten verlenen.

Kopie van een identiteitsbewijs

UWV mag als dit noodzakelijk is voor de identificatie van de betrokkene het identiteitsbewijs verwerken³⁸. Bij het eerste bezoek van een nieuwe klant van UWV aan een UWV-vestiging is UWV bijvoorbeeld verplicht de identiteit van de klant te verifiëren. Dat wordt gedaan door het identiteitsbewijs van de klant te checken. Het is voldoende om in het dossier vast te leggen dat de identiteit is geverifieerd en hoe dit is gedaan. Dit doet de medewerker door het soort document, documentnummer en geldigheidsduur te registreren. Het is in deze situatie niet toegestaan om een kopie van het identiteitsbewijs te maken en in de UWV-systemen (bijvoorbeeld EA) op te slaan. Dit is voor de verificatie van de identiteit namelijk niet noodzakelijk.

In andere situaties wordt wel een kopie van het identiteitsbewijs van een betrokkene verwerkt:

- Wanneer een betrokkene schriftelijk verzoekt om inzage in, correctie of vernietiging van zijn of haar gegevens, wordt deze gevraagd een kopie van het identiteitsbewijs mee te sturen om vast te stellen dat het de betrokkene is die het verzoek doet. Let op: ook hier mag de kopie uitsluitend voor de ID-check worden gebruikt en niet worden bewaard. Dat de ID-check heeft plaatsgevonden moet worden vastgelegd door het soort document, documentnummer en geldigheidsduur te registreren in de centrale registratie van AVG-verzoeken, waarna de kopie wordt vernietigd. Overigens is het voorkeurskanaal voor verzoeken met betrekking tot de rechten van betrokkenen het webformulier op uwv.nl. Om dit formulier te gebruiken moet betrokkene eerst via DigiD inloggen waardoor zijn identiteit al is vastgesteld en een kopie paspoort niet meer nodig is. Zie hiervoor ook hoofdstuk 9 van het UWV beleidskader en de Handreiking Inzagerecht.
- Als werkgever is UWV op grond van de belastingwet verplicht een kopie van het identiteitsbewijs van zijn werknemers in zijn administratie op te nemen. In deze situatie wordt dus wel een kopie van het identiteitsbewijs bewaard.

Er kunnen zich ook nieuwe situaties voordoen waarin het gewenst is een kopie van een ID-bewijs te verwerken. Dit kan alleen als het noodzakelijk is en er dus geen ander alternatief is dat minder ingrijpend is voor de betrokkene. Als zo'n situatie zich voordoet, dan moet de noodzaak voor het verwerken van een kopie ID-bewijs voorafgaand aan de verwerking via een GEB worden onderbouwd en aan de FG worden voorgelegd. Betrek hier altijd het advies van de privacyjuristen van JZ bij.

Let op! Zoals hierboven ook is opgemerkt is het *verwerken* van een kopie ID-bewijs niet per definitie hetzelfde als het *opslaan* of *bewaren* van een kopie ID-bewijs. In het algemeen zal voor een ID check het vastleggen van het soort document, documentnummer en geldigheidsduur voldoende zijn. De noodzaak voor het *bewaren* van een kopie paspoort moet dan ook extra goed onderbouwd worden.

Wanneer betrokkenen worden gevraagd om een kopie ID-bewijs te verstrekken, moeten zij er op gewezen worden dat de kopie zodanig bewerkt is dat deze niet voor andere doeleinden is te gebruiken (ter voorkoming van fraude). Zie hiervoor ook: <https://www.rijksoverheid.nl/onderwerpen/identiteitsfraude/vraag-en-antwoord/fraude-voorkomen-met-kopie-id-bewijs>

Beveiligingscamera's

De Autoriteit Persoonsgegevens beschouwt camerabeelden van beveiligingscamera's als persoonsgegevens van strafrechtelijke aard.³⁹ De reden is dat deze beelden – ingeval van een incident – bedoeld zijn om te gebruiken in een

³⁸ Artikel 25 sub (a) UAVG

³⁹ Beleidsregels Cameratoezicht, Autoriteit Persoonsgegevens, Stcrt. 2016, nr. 4971.

strafrechtelijk onderzoek. Daarom moet bij de verwerking van beelden van beveiligingscamera's wel getoetst worden of er een uitzondering is om deze beelden te verwerken. Zie hiervoor paragraaf 5.2.

Als werkgever mag UWV beveiligingscamera's gebruiken als dit noodzakelijk is om de veiligheid van de medewerkers te verzekeren. Dat kan UWV doen op de grondslag van gerechtvaardigd belang (zie paragraaf 4.4). Wel moet de overweging worden gemaakt of er niet minder ingrijpende middelen zijn om die veiligheid te garanderen. Ook moet ervoor worden gezorgd dat de inbreuk zo klein mogelijk wordt gehouden, bijvoorbeeld door alleen beeld en geen geluid op te nemen, de bewaartermijn zo kort mogelijk te houden en ervoor te zorgen dat de toegang tot die beelden beperkt is. Ook moet het voor de personen die door de camera in beeld worden gebracht duidelijk zijn dat van hen camerabeelden worden gemaakt.

UWV heeft een Protocol videocameratoezicht waarin een nadere uitwerking wordt gegeven van het gebruik van cameratoezicht door UWV (*Videocameratoezichtprotocol versie 1.0 vastgesteld op 31-7-2019 door het MT Huisvesting en Facilitair van Facilitair Bedrijf*). Voor de volledigheid wordt nog opgemerkt dat er betrokkenheid moet zijn van de ondernemingsraad bij het besluit cameratoezicht toe te passen waarbij werknemers in beeld kunnen worden gebracht.

UWV maakt in principe zelf geen gebruik van heimelijk cameratoezicht. Dit betekent dat waar door UWV beveiligingscamera's worden ingezet, de aanwezigheid daarvan duidelijk kenbaar moet zijn voor de personen die door die camera's in beeld worden gebracht.

5.1.3. Andere bijzondere persoonsgegevens

Hoewel UWV hier niet expliciet naar vraagt, komen bijzondere persoonsgegevens betreffende religieuze en levensbeschouwelijke opvattingen in de dienstverlening van UWV soms wel naar voren. Het gaat dan bijvoorbeeld om klanten die op basis van hun *geloof of overtuigingen* bepaalde werkzaamheden niet als arbeid willen aanvaarden. Voorbeelden hiervan zijn een overtuigd veganist die niet in de vleesverwerkingsindustrie wil werken, of een persoon die vanwege zijn of haar religie niet op zondag wil werken. Uit artikel 24 lid 3 Werkloosheidswet en de richtlijn 'passende arbeid' volgt dat er voor werklozen in uitzonderlijke situaties ruimte bestaat om aangeboden arbeid te weigeren op grond van gewetensbezwaren. Voor het succesvol bemiddelen van de klant kan het wenselijk zijn om het gewetensbezwaar vast te leggen zodat geen werk wordt aangeboden dat de klant zal weigeren. De verwerking van dit bijzondere persoonsgegeven is echter alleen toegestaan op grond van de uitdrukkelijke toestemming van de klant, waarbij het hem duidelijk is welke consequenties zijn toestemming hebben (namelijk dat het bijzondere persoonsgegeven in zijn dossier wordt vastgelegd). De algemene grondslag voor de verwerking van persoonsgegevens is in dit geval dat het noodzakelijk is voor uitvoering van wettelijke taak, maar het verbod op de verwerking van persoonsgegevens betreffende religieuze en levensbeschouwelijke opvattingen kan alleen doorbroken worden door de uitdrukkelijke toestemming van de klant. Aangezien het vragen om toestemming in de (afhankelijkheids)relatie tussen UWV en de klant problematisch is, mogen details over de religieuze of levensbeschouwelijke opvattingen van de klant niet in het dossier worden vastgelegd. Het enkele feit dat de klant wegens gewetensbezwaren bijvoorbeeld niet op zondag voor werk beschikbaar is mag dus wel worden vastgelegd, maar het vermelden van de religieuze denominatie is niet toegestaan.

UWV vergoedt een bijdrage aan het lidmaatschap van vakbonden die de cao hebben ondertekend. Dit betekent dat van medewerkers die gebruik maken van deze tegemoetkoming dit bijzondere persoonsgegeven wordt verwerkt. Alleen wanneer de betrokken medewerkers hiervoor uitdrukkelijk zijn toestemming heeft gegeven, mag UWV dit bijzondere persoonsgegeven verwerken. Het vragen van toestemming is in dit geval geen probleem omdat het gaat om de uitvoering van een verzoek dat de medewerker zelf doet en in zijn voordeel is. Maar bij de procedure voor de aanvraag van deze vergoeding zal wel moeten zijn verzekerd dat de medewerker uitdrukkelijk toestemming verleent voor het verwerken van dit bijzondere persoonsgegeven. Die toestemming kan niet impliciet worden aangenomen door het doen van de aanvraag.

Binnen UWV bestaan verschillende netwerken van medewerkers die zich rondom een bepaald thema verenigen. Denk bijvoorbeeld aan Roze Werkt (netwerk van LHBT-collega's) en LEF (netwerk voor culturele diversiteit). De registratie van medewerkers die zich bij een dergelijke netwerk aansluiten, kan ertoe leiden dat bijzondere persoonsgegevens betreffende seksuele gerichtheid of etnische afkomst worden verwerkt. Om dergelijke gegevens rechtmatig te kunnen verwerken is het van belang dat de leden van een dergelijk netwerk uitdrukkelijk toestemming hebben gegeven voor de verwerking van hun persoonsgegevens en het doel van de verwerking

precies is omschreven.⁴⁰ Het netwerk zelf (het bestuur) is verantwoordelijk voor de verwerking van de persoonsgegevens van zijn leden. De verwerking geschiedt dus niet door UWV, maar door het netwerk zelf. Voor zover UWV de administratie van deze netwerken faciliteert, is daarom van belang dat de ledenregistratie goed is beveiligd en op geen enkele wijze toegankelijk is voor medewerkers van HRM of andere medewerkers van UWV.

Overige bijzondere persoonsgegevens, te weten persoonsgegevens betreffende politieke opvattingen, biometrische gegevens met tot doel de unieke identificatie van een persoon en genetische gegevens worden niet door UWV verwerkt.

5.1.4. UWV beleidskader bijzondere persoonsgegevens

Gezondheidsgegevens

■ Medewerkers van UWV mogen op grond van de (U)AVG gezondheidsgegevens verwerken, alleen voor zover dit noodzakelijk is voor:

- a. de uitvoering van wettelijke regelingen (zoals de sociale zekerheidswetten) die verband houden met recht op uitkering of op andere aanspraken in verband met de gezondheidstoestand van de betrokkene; of
- b. re-integratie en arbeidsbemiddeling van zieke of arbeidsongeschikte werknemers of uitkeringsgerechtigden.

■ Gezondheidsgegevens worden binnen UWV uitsluitend gedeeld indien dit noodzakelijk is voor de hiervoor onder a) en b) omschreven wettelijke taken.

■ De verwerking van gezondheidsgegevens in het kader van een beoordeling die tot de specifieke deskundigheid van een verzekeringsarts behoort, mag alleen plaatsvinden door of onder verantwoordelijkheid van een verzekeringsarts.

Foto's, kopie ID en camerabeelden

■ Indien UWV foto's van personen wil verwerken, wordt nagegaan of deze gelet op het doel en de context als bijzondere persoonsgegevens moeten worden aangemerkt. Als dat het geval is, mogen de foto's alleen worden verwerkt indien er een grondslag voor is (zie hoofdstuk 4) en tevens een geldige uitzonderingsgrond.

■ UWV mag alleen een kopie van het identiteitsbewijs vastleggen:

- van de medewerkers in de loonadministratie op grond van de belastingwetgeving.

■ Het publiceren van foto's van collega's in een lokaal smoelenboek of van een bedrijfsuitje op intranet, gebeurt alleen wanneer de desbetreffende collega('s) hiervoor toestemming hebben gegeven.

■ Beveiligingscamera's kunnen worden geplaatst, indien dit noodzakelijk is om de desbetreffende plaats adequaat te kunnen beveiligen. Cameraopnames worden niet langer bewaard dan strikt noodzakelijk is voor het doel en worden daarna vernietigd. Er worden geen opnamen van geluid gemaakt. Aan betrokkenen wordt duidelijk gemaakt dat gebruik wordt gemaakt van beveiligingscamera's.

■ Voor het gebruik van beveiligingscamera's en de verwerking van de camerabeelden is een protocol opgesteld.

■ Filmopnamen voor bijvoorbeeld communicatiedoeleinden, opleidingen of van bedrijfsuitjes mogen alleen op basis van vrijwilligheid worden gemaakt.

Andere bijzondere persoonsgegevens

⁴⁰ Artikel 9 lid 2 sub (a) AVG en artikel 22 lid 2 onder a UAVG.

- UWV kan bepaalde categorieën van bijzondere persoonsgegevens verwerken, indien en voor zover de AVG en de UAVG hiervoor een uitzondering bieden.
- Indien UWV van een klant of andere betrokkene bijzondere persoonsgegevens verwerkt, wordt de betrokkene hierover altijd geïnformeerd, bijvoorbeeld via een privacyverklaring.
- In het register van verwerkingen wordt aangegeven in welke verwerkingen bijzondere persoonsgegevens worden verwerkt.
- Persoonsgegevens betreffende religieuze of levensbeschouwelijke overtuigingen mogen door UWV niet worden verwerkt. Wel mag in het kader van passende arbeid worden geregistreerd dat een klant gewetensbezwaren heeft.
- Persoonsgegevens over het lidmaatschap van een vakbond verwerkt UWV uitsluitend van medewerkers die hebben verzocht om een financiële vergoeding van hun lidmaatschap van een vakbond en hun toestemming hebben gegeven voor de noodzakelijke verwerking van deze gegevens.
- In het kader van de netwerken van medewerkers binnen UWV kunnen bijzondere persoonsgegevens uitsluitend worden verwerkt na uitdrukkelijke toestemming van medewerkers die zich bij dat netwerk wensen aan te sluiten. De verwerking van deze persoonsgegevens geschiedt onder verantwoordelijkheid van het bestuur van het netwerk (en dus niet door UWV).

5.2. Persoonsgegevens van strafrechtelijke aard

Wat zegt de AVG?

Gegevens over een persoon van strafrechtelijke aard, zoals bijvoorbeeld over een eerdere strafrechtelijke veroordeling van die persoon, het uitzitten van een gevangenisstraf, strafbare feiten waarmee die persoon in verband is gebracht of bepaalde veiligheidsmaatregelen die aan die persoon zijn opgelegd (bijv. een contactverbod), mogen niet zomaar worden verwerkt. Dit mag alleen onder toezicht van de overheid of indien dit door de wet (de UAVG) is toegestaan.

Artikel 10 AVG, artikel 31 t/m 33 UAVG

Persoonsgegevens van strafrechtelijke aard zijn extra gevoelig. Ze zeggen iets over het feit dat een persoon in verband wordt gebracht met het plegen van een strafbaar feit. Bijvoorbeeld omdat hij als verdachte betrokken was bij een strafbaar feit of omdat hij voor een strafbaar feit veroordeeld is tot een (gevangenis)straf. De verwerking van deze informatie kan negatieve gevolgen hebben voor de desbetreffende persoon, zoals het stempel 'crimineel' dat hem kan blijven achtervolgen. Daarom mogen gegevens van strafrechtelijke aard alleen worden verwerkt als er in aanvulling op de grondslag voor de verwerking van persoonsgegevens (zie hoofdstuk 5) ook sprake is van één van de in de UAVG genoemde uitzonderingsgevallen.

UWV verwerkt in bepaalde gevallen gegevens van strafrechtelijke aard. Zo wordt door de divisies Gegevensdiensten en Uitkeren bijvoorbeeld geregistreerd of een persoon is gedetineerd omdat dit van invloed is op zijn uitkering. Dergelijke persoonsgegevens van strafrechtelijke aard mogen door UWV worden verwerkt op grond van artikel 33 lid 1 onder a UAVG. Deze gegevens heeft UWV namelijk vanuit politie of justitie ontvangen voor specifieke taken die aan UWV zijn opgedragen in de wet. In dit geval zijn de gegevens noodzakelijk om te bepalen of de betrokkene recht heeft op een uitkering.

Ook kan een eerdere veroordeling of een opgelegde veiligheidsmaatregel (zoals bijvoorbeeld een door de rechter opgelegde beperking dat een persoon een aantal jaren niet in een bepaalde sector werkzaam mag zijn) relevant zijn in het kader van de taken van UWV op het terrein van re-integratie en arbeidsbemiddeling. Ook deze gegevens kunnen worden verwerkt op grond van artikel 33 lid 1 onder a UAVG.

Als overheidswerkgever mag UWV op grond van artikel 33 lid 1 onder a UAVG strafrechtelijke gegevens verwerken van kandidaten voor een positie bij UWV als dit nodig is om de bekwaamheid en geschiktheid te beoordelen (screening) (artikel 4, Uitvoeringsbesluit Ambtenarenwet 2017, Stb. 2019, 346). Het gaat hierbij om de Verklaring omtrent gedrag (VOG) en indien alleen een VOG onvoldoende is, ook om bepaalde andere strafrechtelijke gegevens. In dat geval moet wel worden gemotiveerd waarom niet met een VOG kan worden volstaan. Een VOG op zichzelf bevat geen persoonsgegevens van strafrechtelijke aard, maar het feit dat een VOG is afgewezen is wel een persoonsgegeven van strafrechtelijke aard en moet dus als zodanig worden behandeld. De verwerking van gegevens van strafrechtelijke aard door een werkgever moet bovendien in overeenstemming zijn met de bepalingen van de Wet op de ondernemingsraden.⁴¹

Camerabeelden van beveiligingscamera's worden door de Autoriteit Persoonsgegevens aangemerkt als gegevens van strafrechtelijke aard omdat ze bedoeld zijn om te worden gebruikt door de politie na een incident (zie ook paragraaf 5.1.2). UWV mag deze gegevens verwerken op basis van de uitzonderingsgrond neergelegd in artikel 33 lid 2 onder b UAVG.⁴²

Of een persoon agressief gedrag heeft vertoond, is wel een persoonsgegeven, maar op zichzelf geen persoonsgegeven van strafrechtelijke aard. Dit is relevant in verband met Agressie Registratie Overheid (ARO). In de ARO worden geen strafrechtelijke gegevens verwerkt.

Er is nog een aantal situaties waarin UWV strafrechtelijke gegevens verwerkt. Omdat voor elk van deze situaties een andere uitzonderingsgrond kan gelden, is het advies om de privacyjuristen van JZ te betrekken bij het onderbouwen van de rechtmatigheid van deze verwerkingen.

Verwerking van persoonsgegevens door de Directie Handhaving

Door de Directie Handhaving worden persoonsgegevens verwerkt in het kader van onderzoeken naar uitkeringsfraude. Dit zijn meestal bestuursrechtelijke onderzoeken. De persoonsgegevens die de Directie Handhaving verwerkt in het kader van deze bestuursrechtelijke onderzoeken vallen onder de AVG. Het komt echter ook voor dat wordt besloten een strafrechtelijk traject te bewandelen. In dat geval is sprake van een strafrechtelijk onderzoek dat is gericht op opsporing en vervolging, onder gezag van de officier van justitie. De persoonsgegevens die worden verwerkt in het kader van zo'n strafrechtelijk opsporingsonderzoek vallen niet onder de AVG, maar onder de Wet politiegegevens.⁴³ Bij de Directie Handhaving werken een aantal buitengewoon opsporingsambtenaren (boa's) die opsporingsbevoegdheid hebben. Zij houden zich bezig met dergelijke strafrechtelijke onderzoeken.

Van belang is dat de verwerking van dergelijke opsporingsgegevens in de systemen niet alleen goed is beveiligd, maar ook is afgescheiden van andere verwerkingen. Alleen de buitengewoon opsporingsambtenaren zijn bevoegd hiervan kennis te nemen.

UWV beleidskader

- **UWV verwerkt persoonsgegevens van strafrechtelijke aard indien deze noodzakelijk zijn voor het vaststellen van het uitkeringsrecht (bijvoorbeeld gegevens betreffende de detentie van uitkeringsgerechtigden).**
- **UWV kan als werkgever gegevens van strafrechtelijke aard verwerken voor screeningsdoeleinden, maar alleen als een VOG niet volstaat.**
- **Camerabeelden van beveiligingscamera's gelden ook als strafrechtelijke gegevens. Deze mag UWV verwerken op grond van artikel 33 lid 2 onder b UAVG.**

⁴¹ Artikel 33 lid 3 UAVG.

⁴² De gegevens worden verwerkt ter bescherming van de belangen van UWV, voor zover het gaat om strafbare feiten die zijn of op grond van feiten en omstandigheden naar verwachting zullen worden gepleegd tegen UWV of tegen medewerkers van UWV.

⁴³ In de Wet politieregisters is de Europese Richtlijn gegevensbescherming opsporing en vervolgen (2016/680, PbEU 2016, L 119) geïmplementeerd. Deze richtlijn is de evenknie van de AVG voor de bescherming van persoonsgegevens die worden verwerkt in het kader van de strafrechtelijke handhaving (opsporing en vervolging).

■ **Persoonsgegevens die worden verwerkt door Directie Handhaving in het kader van een strafrechtelijk onderzoek, worden afgescheiden van andere verwerkingen van UWV. Alleen de buitengewoon opsporingsambtenaren hebben hiertoe toegang.**

5.3. Burgerservicenummer (BSN)

Wat zegt de AVG en de UAVG?

Lidstaten mogen specifieke regels opstellen voor het gebruik van een nationaal identificatienummer. Het burgerservicenummer (BSN) is zo'n nationaal identificatienummer. Nederland heeft hiervoor specifieke regels opgesteld. Het BSN is bedoeld voor de overheid en mag alleen door private partijen worden verwerkt als daarvoor in de wet een uitzondering is gemaakt.

Artikel 87 AVG, artikel 46 UAVG, artikel 10 Wabb, Zie ook Handleiding gebruik BSN UWV

Het BSN is destijds ingevoerd met als doel één uniform persoonsnummer voor de overheid te introduceren, zowel voor de communicatie tussen overheid en burger als voor de uitwisseling van gegevens tussen overheidsorganisaties onderling. Vóór invoering gebruikte de overheid naast het sofi-nummer nog een aantal andere persoonsnummers, afhankelijk van het onderwerp. Om redenen van uniformiteit en doelmatigheid en om de kans op fouten bij verwerking van persoonsgegevens van burgers door de overheid te verminderen, werd het BSN ingevoerd. Het BSN is dus bedoeld voor de overheid en daarom mogen private partijen het BSN in principe niet gebruiken en vastleggen, tenzij de wet daarvoor een uitzondering heeft gemaakt. Zo'n uitzondering geldt bijvoorbeeld voor de gezondheidszorg (bijv. artsen, ziekenhuizen, apotheken) en werkgevers in de loonadministratie.

Omdat het BSN kan worden gebruikt om verschillende bestanden aan elkaar te koppelen, kan hierdoor vrij eenvoudig heel veel informatie over een persoon worden verzameld waardoor een uitgebreid beeld van zijn of haar privéleven ontstaat. Daarnaast kan misbruik van het BSN leiden tot identiteitsfraude met zeer negatieve gevolgen voor de betrokkene. De verwerking van het BSN is dan ook aan strikte regels gebonden. Het verwerken van het BSN is alleen toegestaan als daarvoor een wettelijke basis bestaat. Het verbod om het BSN te gebruiken kan niet worden doorbroken door het vragen van toestemming aan de betrokkene voor het gebruik van diens BSN. Daarnaast moet (ook) bij de verwerking van het BSN steeds worden afgewogen in hoeverre het gebruik van het BSN echt noodzakelijk is en of er in redelijkheid niet een minder privacyschendend alternatief is voor het gebruik van het BSN. Als het gebruik van het BSN niet echt noodzakelijk is en als er in redelijkheid een minder privacyschendend alternatief is, dan is het verwerken van het BSN niet toegestaan.

UWV is een overheidsorganisatie die op grond van artikel 10 Wet algemene bepalingen burgerservicenummer (Wabb) bevoegd is het BSN te verwerken voor zover dit noodzakelijk is voor de uitvoering van zijn wettelijke taken. Binnen UWV wordt het BSN op dit moment vrij uitgebreid verwerkt. Voor veel systemen is het BSN hét koppelgegeven waarmee persoonsgegevens uit verschillende bestanden kunnen worden gekoppeld.

Omdat binnen UWV veel vragen bestaan over het gebruik van BSN, is een *Handleiding gebruik BSN UWV* (zie link in bijlage) opgesteld. In de handleiding wordt ingegaan op de vraag in welke gevallen en onder welke voorwaarden het BSN mag worden verwerkt. Dit beleidskader beperkt zich daarom tot enkele hoofdlijnen en verwijst verder naar de handleiding.

Ten aanzien van het BSN van medewerkers van UWV geldt voor UWV als werkgever kort gezegd het volgende:

- UWV is verplicht het BSN van zijn medewerkers te gebruiken in de loonadministratie voor het doel van uitwisseling van loongegevens met de Belastingdienst.
- UWV gebruikt het BSN van zijn medewerkers ten behoeve van de re-integratie van medewerkers van UWV.

Ten aanzien van het BSN van klanten van UWV, is UWV bevoegd het BSN in de uitwisseling met andere partijen te gebruiken:

- In de communicatie met de *klant*, maar dan alleen als dit noodzakelijk is en uitsluitend het BSN van die betreffende klant.
- Bij de uitwisseling van persoonsgegevens met *overheidsorganen* (bijv. Belastingdienst, gemeenten, SVB), voor zover dat past binnen het doel waarvoor die derde (het andere overheidsorgaan) het BSN mag gebruiken, tenzij er sprake is van omstandigheden waarin het gebruik van het BSN onwenselijk is.
- Bij de uitwisseling van persoonsgegevens met andere (private) organisaties, voor zover die organisaties werkzaamheden verrichten waarbij het gebruik van het BSN bij of krachtens de wet is voorgeschreven en de uitwisseling past binnen die werkzaamheden.
- Bij de uitwisseling van persoonsgegevens tussen UWV en een werkgever met betrekking tot een werknemer van die werkgever.

Gezien de gevoeligheid van het gegeven dient UWV bij het gebruik van het BSN uiteraard altijd passende waarborgen te nemen en het gegeven adequaat te beveiligen.

UWV beleidskader

- **UWV mag het BSN van klanten verwerken als dit noodzakelijk en proportioneel is voor de uitvoering van zijn wettelijke taken. Dit betekent dat het BSN van de klant ook mag worden gebruikt in de communicatie met die klant.**
- **Als werkgever is UWV voor bepaalde taken verplicht of bevoegd het BSN van zijn medewerkers verwerken.**
- **In de samenwerking met andere overheidsorganisaties mag UWV het BSN verstrekken als dit nodig is om de identificatie van de desbetreffende persoon te verzekeren in het kader van de uitvoering van de wettelijke taak.**
- **De uitwisseling van het BSN met een private partij is alleen toegestaan indien de private partij een wettelijke basis heeft voor het gebruik van het BSN en de uitwisseling van het BSN hierin past.**

5.4. Verwerking van spontaan verstrekte persoonsgegevens

De meeste persoonsgegevens die UWV verwerkt, zijn persoonsgegevens die UWV doelgericht verzamelt bij bijvoorbeeld een klant, werkgever, medewerker of een andere organisatie ten behoeve van een specifiek verwerkingsdoel. Zoals in de voorgaande paragrafen is aangegeven, kan dat voor bepaalde doeleinden ook gaan om bijzondere persoonsgegevens en persoonsgegevens van strafrechtelijke aard. Dergelijke gegevens worden alleen bij de klant of een derde uitgevraagd door die medewerkers die bevoegd zijn dergelijke gegevens te verwerken en er is vooraf al nagedacht over welke gegevens precies nodig zijn.

Het komt echter ook voor dat klanten ongevraagd en dus spontaan gegevens aan UWV verstrekken omdat ze van oordeel zijn dat die gegevens relevant zijn voor hun dossier. Om dit te kunnen beoordelen zullen de gegevens moeten worden vastgelegd en onderdeel uitmaken van het dossier. Dit vastleggen is bovendien van belang vanuit het perspectief van de archiefwetgeving. Echter, het kan hierbij ook om bijzondere persoonsgegevens of persoonsgegevens van strafrechtelijke aard gaan. Als dergelijke gegevens ontvangen worden door een medewerker die niet bevoegd is om die gegevens te verwerken, stuurt die medewerker de gegevens door naar de afdeling die hiertoe wel bevoegd is. Als een klant bijvoorbeeld spontaan gezondheidsgegevens met een vertrouwelijkheidsklasse 3 verstrekt aan een medewerker die niet bevoegd is deze te verwerken, worden deze gegevens meteen doorgezonden naar SMZ. De gegevens worden ook niet bewaard door de medewerker die deze heeft ontvangen.

In het kader van privacy by design is het de bedoeling de processen zo in te richten en toe te lichten dat de kans zo klein mogelijk wordt dat klanten spontaan ongevraagde bijzondere persoonsgegevens verstrekken. Voorbeeld hiervan is dat het gebruik van vrije tekstvelden in de klantportalen zoveel mogelijk moet worden vermeden. Een afzonderlijke categorie van spontaan verstrekte persoonsgegevens zijn de fraudemeldingen die door burgers, werkgevers en medewerkers van UWV kunnen worden gedaan. Hiervoor heeft UWV een centraal

meldpunt fraude ingericht. Wil iemand een vermoeden van fraude melden, dan kan hij of zij worden doorverwezen naar het meldpunt en de bestaande procedures voor het melden van fraude.⁴⁴

5.5. Ontvangen en verzamelen van persoonsgegevens

De persoonsgegevens die UWV verwerkt, ontvangt UWV op verschillende manieren en op basis van verschillende wettelijke bepalingen.

Een belangrijke bron is uiteraard de betrokkene zelf. Klanten van UWV verstrekken persoonsgegevens die UWV nodig heeft om bijvoorbeeld een uitkeringsaanvraag te beoordelen, een sociaal-medische beoordeling te kunnen opstellen of te helpen een baan te vinden. Nieuwe medewerkers van UWV of externe medewerkers die door UWV worden ingehuurd, verstrekken aan UWV hun persoonsgegevens.

Daarnaast ontvangt UWV ook veel gegevens van derden. Dit kan zijn omdat die derde op grond van de wet verplicht is bepaalde persoonsgegevens aan UWV te leveren ('leverplicht') of omdat deze daartoe bevoegd is.⁴⁵ Het kan gaan om structurele levering, bijvoorbeeld de verplichting van werkgevers bepaalde gegevens over hun werknemers aan UWV te verstrekken of om incidentele verstrekking. In paragraaf 5.1.1 over gezondheidsgegevens is een aantal voorbeelden van incidentele verstrekking van gezondheidsgegevens aan UWV besproken. Een ander voorbeeld van het incidenteel ontvangen van persoonsgegevens van derden is het geval waarin DHH gegevens van een externe partij vordert in het kader van een bestuursrechtelijk fraudeonderzoek.

5.6. Delen en verstrekken van persoonsgegevens

Wat zeggen de AVG en de Wet SUWI?

Het delen en verstrekken van persoonsgegevens is een vorm van verwerken van persoonsgegevens en moet dus aan de eisen van de AVG voldoen. In het bijzonder moet worden gedacht aan de eisen van rechtmatigheid (grondslag), doelbinding en proportionaliteit. Bovendien geldt op grond van de Wet SUWI dat alleen persoonsgegevens aan derden mogen worden verstrekt voor zover dat noodzakelijk is ter uitvoering van die wet of is toegestaan op basis van een wettelijke bepaling. De verstrekking van persoonsgegevens is ook toegestaan met de toestemming van betrokkene (m.u.v. het BSN).

Artikel 4 onder 2 AVG en artikel 74 Wet SUWI, Instructie Gegevensverstrekking Aan Derden (IGAD)

De grote hoeveelheid persoonsgegevens waar UWV over beschikt vormt een aantrekkelijke bron van informatie voor derden. UWV ontvangt dan ook veel verzoeken van andere organisaties om persoonsgegevens te verstrekken. Het kan gaan om (overheids)organisaties die de persoonsgegevens nodig hebben voor de uitvoering van hun taken (bijv. gemeenten, gerechtsdeurwaarders of pensioenfondsen), maar ook om verzoeken van wetenschappers om onderzoek te mogen doen op basis van de gegevens waarover UWV beschikt.

Ook intern binnen UWV bestaat de behoefte om gegevens tussen divisies of afdelingen te delen, bijvoorbeeld omdat de eigen doelsystemen onvoldoende voorzien in de behoefte om bepaalde overzichten te creëren.

Binnen UWV worden verschillende termen gebruikt voor het beschikbaar stellen van gegevens aan een ander. Het 'verstrekken' of 'delen' van gegevens zijn algemeen gebruikte termen. De divisie Gegevensdiensten gebruikt doorgaans de term 'leveren' van gegevens. De term 'delen' van persoonsgegevens wordt vaak gebruikt als persoonsgegevens in één doelsysteem of applicatie beschikbaar worden gesteld aan verschillende partijen (denk aan Sonar). Ook het (laten) inzien van persoonsgegevens op een UWV-kantoor, bijvoorbeeld door een derde te autoriseren voor een bepaald systeem of bestand, is een vorm van verstrekking van gegevens. Vanuit juridisch perspectief is het allemaal hetzelfde. Het gaat erom dat de persoonsgegevens aan een ander beschikbaar worden gesteld. Hoe dat technisch gebeurt - bijvoorbeeld door een bestand met gegevens te verstrekken of door de andere partij toegang te geven tot een systeem waarin de desbetreffende gegevens staan - maakt voor de AVG niet uit.

⁴⁴ <https://digitalewerkplek.sharepoint.uwv.nl/werkprocessen/Paginas/als-je-vermoedt-dat-iemand-zich-niet-aan-de-regels-houdt.aspx>

⁴⁵ Bijv. op basis van artikel 54 Wet SUWI.

5.6.1. Verstrekken van persoonsgegevens aan externe partijen

Het is niet eenvoudig om in enkele paragrafen een sluitend beeld te schetsen van de gevallen waarin UWV bevoegd is om persoonsgegevens te verstrekken aan organisaties buiten UWV. Dit hangt onder andere af van de organisatie die de gegevens wil hebben, het doel waarvoor ze worden gevraagd en om welke gegevens het gaat. Een wirwar aan wettelijke bepalingen vormt het geheel aan regels over de gevallen waarin gegevens met derden mogen worden gedeeld en welke gegevens dat betreft. Het gaat zowel om incidentele verzoeken als om systematische verstrekking (levering) van persoonsgegevens, bijvoorbeeld op basis van een zogenoemd abonnement. Gegevensdiensten houdt een overzicht bij van alle grondslagen op basis waarvan UWV persoonsgegevens kan verstrekken aan andere partijen.

Verstrekking van persoonsgegevens van klanten is uitsluitend toegestaan als dit noodzakelijk is voor de uitvoering van de wettelijke taak van UWV of als UWV wettelijk verplicht is de gegevens te verstrekken. Als hiervan geen sprake is, kan in uitzonderlijke gevallen en na raadpleging van Juridische Zaken verstrekking mogelijk zijn met toestemming van de klant. Uiteraard geldt in al deze situaties dat de partij aan wie de gegevens worden verstrekt zelf ook over een grondslag moet beschikken om deze gegevens te ontvangen en verder te verwerken.

Hoofdregel: verstrekking aan derden geschiedt door of na raadpleging van de divisie Gegevensdiensten

Omdat het van belang is te verzekeren dat UWV uitsluitend gegevens deelt met derden als daar een wettelijke grondslag voor bestaat en dit voldoet aan de beginselen van doelbinding en proportionaliteit, geldt als hoofdregel dat alle verstrekkingen van gegevens (ook wel gegevensleveringen genoemd) plaatsvinden door of na raadpleging van de divisie Gegevensdiensten. Bij de divisie Gegevensdiensten werken specialisten (wetstechnisch adviseurs) met kennis van de relevante regelgeving die in staat zijn te beoordelen of het delen/verstrekken/leveren van bepaalde gegevens in het concrete geval rechtmatig is. Door verstrekking van persoonsgegevens via de divisie Gegevensdiensten te laten verlopen, wordt rechtmatigheid, uniformiteit en zorgvuldigheid verzekerd. De Instructie gegevensverstrekking aan derden (IGAD)⁴⁶ geeft inzicht in hoe de divisie Gegevensdiensten gegevensverstrekkingen heeft georganiseerd en hoe gegevensleveringen worden getoetst.

Het uitgangspunt dat de divisie Gegevensdiensten de verstrekking van persoonsgegevens aan derden toetst, betekent dat wanneer een medewerker wordt benaderd met een verzoek van een persoon of organisatie buiten UWV om bepaalde persoonsgegevens aan diegene te verstrekken, de verzoeker wordt doorverwezen naar de divisie Gegevensdiensten of het verzoek voor toetsing aan Gegevensdiensten wordt voorgelegd. Dit geldt zeker wanneer het gaat om grootschalige verstrekking van gegevens (bulklevering). Dit geldt dus ook voor organisatieonderdelen die zelf toegang hebben tot grote hoeveelheden persoonsgegevens, bijvoorbeeld in het kader van een analyseomgeving.

Op het uitgangspunt dat alle verstrekkingen van persoonsgegevens via de divisie Gegevensdiensten moeten verlopen, bestaan, omwille van de uitvoerbaarheid, wel drie uitzonderingen:

- a) Verstrekken van persoonsgegevens aan derden in het kader van een specifiek geval of dossier;
- b) Verstrekking van persoonsgegevens via Suwinet;
- c) Verstrekken van persoonsgegevens aan leveranciers voor zover de leverancier de persoonsgegevens nodig heeft voor het uitvoeren van de opdracht die hij van UWV heeft gekregen.

Op het intern delen van persoonsgegevens met collega's binnen UWV wordt in paragraaf 5.6.2 verder ingegaan.

Ad a) Verstrekken van persoonsgegevens aan derden in verband met een specifiek dossier of geval

Medewerkers van UWV hebben in hun dagelijks werk vele contacten met externe partijen zoals werkgevers, re-integratiebureaus, gemeenten en andere bedrijven en organisaties. Die contacten gaan in veel gevallen over concrete gevallen waarin gegevens over een concrete klant gedeeld worden. Denk bijvoorbeeld aan het navraag doen bij een werkgever of een sollicitatie van een klant goed is verlopen, een afspraak plannen met een begeleider van een klant of follow up bij een leverancier van een voorziening.

Het is praktisch ondoenlijk wanneer de verstrekking van persoonsgegevens op casus niveau ook door of na raadpleging van de divisie Gegevensdiensten zou moeten plaatsvinden. Hoewel de gegevensverstrekking op gevalsniveau plaatsvindt, is er vaak toch een generiek proces dat daaraan ten grondslag ligt. In die situaties mag

⁴⁶ Te vinden op de Kennispoort via DWU.

dan ook worden verwacht dat werkinstructies medewerkers duidelijkheid verschaffen hoe met de verstrekking moet worden omgegaan. Is er geen werkinstructie waar de medewerker op kan terugvallen, dan wordt geadviseerd om de BSO te raadplegen. In ieder geval zullen voor de verstrekking steeds de volgende vragen moeten worden beantwoord:

- Is er een grondslag voor de verstrekking? Is de verstrekking bijvoorbeeld noodzakelijk voor de uitvoering van de wettelijke taak van de ontvanger?
- Voldoet de verstrekking aan het beginsel van doelbinding? Is het doel van de verstrekking gelijk aan het doel waarvoor UWV de gegevens heeft verzameld of is het daarmee verenigbaar op basis van de aspecten die in artikel 6.4 AVG worden benoemd? (zie ook paragraaf 3.3)
- Worden uitsluitend die gegevens verstrekt die noodzakelijk zijn?

Ad b) Verstrekking van persoonsgegevens via Suwinet

Suwinet is een elektronische voorziening die primair voor UWV, de SVB en gemeenten is bedoeld om gemakkelijk gegevens uit te wisselen. Naast deze drie partijen zijn inmiddels ook andere overheidsorganisaties aangesloten op Suwinet, zoals DUO en het Kadaster. BKWI is de beheerder van Suwinet en verleent de autorisaties voor de toegang tot Suwinet, nadat de betrokken verwerkingsverantwoordelijke het verzoek om gegevens heeft getoetst. Gegevensdiensten toetst dergelijke verzoeken als het gaat om gegevens waarvoor UWV verwerkingsverantwoordelijke is. Dit betekent dat voor verstrekkingen van klantgegevens via Suwinet reeds een toets door Gegevensdiensten heeft plaatsgevonden. Er is dan geen toets voor de daadwerkelijke verstrekking via Suwinet meer nodig.

Ad c) Verstrekking van persoonsgegevens aan een leverancier

Een leverancier die persoonsgegevens verwerkt in het kader van de uitvoering van een opdracht van UWV kan dit doen in de hoedanigheid van verwerkingsverantwoordelijke of van verwerker (zie paragraaf 2.3).

Indien de leverancier verwerker is, dan is er indien hij persoonsgegevens van UWV ontvangt geen sprake van een verstrekking aan een derde, zoals hierboven bedoeld. Een verwerker verwerkt de persoonsgegevens in opdracht en onder verantwoordelijkheid van UWV. De persoonsgegevens komen dus niet buiten de macht van UWV. Voor zover de verwerker de persoonsgegevens nodig heeft voor de uitvoering van zijn opdracht (het verwerken van persoonsgegevens is juist zijn opdracht) mogen deze gegevens dus aan de verwerker worden verstrekt.

Indien de leverancier verwerkingsverantwoordelijke is, dan is er in het geval UWV aan hem persoonsgegevens verstrekt, wel sprake van een verstrekking aan een derde. Indien de leverancier wordt ingeschakeld bij de uitvoering van de wettelijke taak van UWV (bijv. het verstrekken van een aangepaste computer aan een uitkeringsgerechtigde in het kader van een voorziening), dan is het aan die leverancier verstrekken van persoonsgegevens die de leverancier nodig heeft voor het uitvoeren van de opdracht, toegestaan. Indien de leverancier wordt ingeschakeld ten behoeve van de bedrijfsvoering van UWV (bijv. de levering van lease-auto's ten behoeve van UWV-medewerkers), dan is in dat geval het aan die leverancier verstrekken van persoonsgegevens die de leverancier nodig heeft voor het uitvoeren van de opdracht, toegestaan.

Verstrekking aan organisaties in het buitenland

Voor sommige organisatieonderdelen van UWV (zoals SMZ/Bijzondere Zaken en de directie Handhaving) is nog het volgende van belang. Op grond van de AVG gelden extra strenge regels wanneer sprake is van verstrekking (in de AVG 'doorgifte' genoemd) van persoonsgegevens aan organisaties in landen buiten de Europese Economische Ruimte (EER). De EER betreft alle lidstaten van de EU en Noorwegen, IJsland en Liechtenstein. De AVG geldt alleen in de landen die vallen binnen de EER. Verstrekking van persoonsgegevens naar landen buiten de EER, waaronder sinds de Brexit ook Groot Brittanie, is op grond van de AVG niet zomaar toegestaan.

Het is mogelijk om persoonsgegevens door te geven aan landen buiten de EER als:

- een land buiten de EER in de nationale wetgeving een passend niveau van gegevensbescherming biedt. De Europese Commissie (EC) kan dan een 'adequaateitsbeslissing' nemen. De EC stelt dan vast dat de gegevensbescherming in dat land van een vergelijkbaar niveau is als de AVG. Voor Groot Brittanie heeft de EC op 28 juni 2021 een adequaateitsbesluit genomen;
- doorgifte op basis van passende waarborgen plaatsvindt, bijvoorbeeld door middel van een Modelcontract of Gedragscode en certificering;

- doorgifte plaatsvindt op basis van bindende bedrijfsvoorschriften (Binding Corporate Rules, BCR) over privacy, waaraan de medewerkers van een bedrijf zich moeten houden;
- doorgifte plaatsvindt op basis van specifieke uitzonderingen: bijvoorbeeld bij uitdrukkelijke toestemming van betrokkene of bij een verdrag waar Nederland en dat andere land partij bij zijn.

Voor UWV geldt dat verstrekking aan organisaties buiten de EER altijd plaatsvindt op grond van een verdrag dat tussen Nederland en het ontvangende land is afgesloten of waar beide landen partij bij zijn. Raadpleeg bij vragen hierover Juridische Zaken.

5.6.2. Delen van persoonsgegevens met UWV-collega's

Uitgangspunt is dat met collega's wordt gewerkt in doelsystemen. Door middel van het autorisatiebeleid wordt dan verzekerd dat alleen die collega's toegang hebben tot de desbetreffende gegevens die daartoe ook bevoegd zijn op basis van hun taken en functie.

Toch kan het voorkomen dat het nodig is om buiten de doelsystemen om persoonsgegevens met collega's van UWV te delen. Dit mag ook voor zover dit noodzakelijk is voor de uitvoering van de taken. Maar het delen van die gegevens moet wel voldoen aan de in hoofdstuk 4 genoemde beginselen en in het bijzonder die van doelbinding en data-minimalisatie/proportionaliteit. Het is dus niet zo dat alle persoonsgegevens die UWV verwerkt door collega's binnen UWV zonder meer mogen worden uitgewisseld en gedeeld. Het feit dat alle medewerkers van UWV een geheimhoudingsplicht hebben doet hier niets aan af.

Voordat gegevens met een collega worden gedeeld, moet daarom duidelijk zijn:

- met welk doel de persoonsgegevens worden gedeeld;
- of de ontvanger van de persoonsgegevens bevoegd is om van die gegevens kennis te nemen en deze te verwerken;
- dat gegevens alleen voor het desbetreffende doel mogen worden verwerkt;
- dat niet méér gegevens worden gedeeld dan noodzakelijk is voor het doel;
- dat er op een veilige manier wordt omgesprongen met de gegevens;
- Dat de gegevens tijdig worden gearhiveerd en vernietigd.

Overleg tussen de vragende en verstrekkeende collega is van belang om over deze punten duidelijkheid te krijgen.

Idealiter wordt bij een voorgenomen werkproces al vroegtijdig middels een GEB duidelijk dat het een gedeelte van het werkproces niet in doelsystemen kan worden uitgevoerd. De hierboven opgesomde vragen worden dan al voor het in gebruik nemen van het proces beantwoord, zodat in de werkinstructie kan worden opgenomen hoe de betreffende stappen van het werkproces moeten worden uitgevoerd en welke aanvullende maatregelen eventueel nog moeten worden genomen. Op deze manier hoeven medewerkers in de uitvoering niet elke keer opnieuw deze afweging te maken.

Het intern delen van (grote) bestanden van persoonsgegevens uit analyseomgevingen geschiedt centraal door de divisie Gegevensdiensten (zie ook paragraaf 5.7.1).

Verstrekken van persoonsgegevens van medewerkers van UWV aan UWV als uitvoerder van sociale zekerheidswetgeving

UWV verwerkt als werkgever persoonsgegevens van zijn werknemers. UWV is als werkgever, net als alle andere werkgevers in Nederland, verplicht om bepaalde persoonsgegevens aan UWV als uitvoerder van sociale zekerheidswetgeving te verstrekken. Voor de duidelijkheid wordt opgemerkt dat dergelijke verstrekkingen buiten het hierboven omschreven regime vallen. Het gaat om verstrekking van persoonsgegevens van werknemers op basis van een wettelijke verplichting. Ook de divisie Gegevensdiensten speelt bij een dergelijke verstrekking van persoonsgegevens geen rol.

UWV beleidskader

- **Verstrekkingen van persoonsgegevens aan derden dienen altijd te voldoen aan de Instructie gegevensverstrekking aan derden (IGAD).**

- **Als hoofdregel geldt dat verstrekking van persoonsgegevens aan personen of organisaties buiten UWV geschiedt door of na raadpleging van de divisie Gegevensdiensten. Dit geldt altijd wanneer het gaat om verstrekking van grote bestanden (bulkleveringen).**
- **Wanneer een medewerker een verzoek ontvangt voor verstrekking/levering van persoonsgegevens, wordt de verzoeker doorverwezen naar de divisie Gegevensdiensten of wordt het verzoek aan hen voorgelegd.**
- **Van de hoofdregel kan worden afgeweken wanneer het gaat om het verstrekken van persoonsgegevens op casusniveau en hiervoor een grondslag bestaat, de verstrekking van de gegevens noodzakelijk is voor de wettelijke taken van UWV en niet meer gegevens worden verstrekt dan noodzakelijk is voor het doel.**
- **Er gelden speciale regels voor de verstrekking / doorgifte van persoonsgegevens aan organisaties in landen buiten de EER. Voordat persoonsgegevens aan een bedrijf of (zuster)organisatie buiten de EU mogen worden verstrekt, moet eerst worden nagegaan of aan deze speciale regels wordt voldaan. Zo nodig wordt Juridische Zaken hierover geconsulteerd.**
- **Persoonsgegevens binnen UWV worden in beginsel alleen met collega's gedeeld via de daartoe bestemde doelsystemen. Wanneer het nodig is om buiten de doelsystemen om persoonsgegevens met collega's te delen, wordt altijd in overleg met de collega beoordeeld of dit noodzakelijk is en de collega bevoegd is om van de gegevens kennis te nemen. Vervolgens worden niet méér gegevens gedeeld dan noodzakelijk en wordt ervoor gezorgd dat met de gegevens veilig wordt omgesprongen.**
- **Aan een verwerker die ten behoeve van UWV persoonsgegevens verwerkt mogen persoonsgegevens worden verstrekt. De verwerker verwerkt de persoonsgegevens onder verantwoordelijkheid van UWV (verwerkingsverantwoordelijke). Daarom is geen sprake van een verstrekking buiten de macht van de verwerkingsverantwoordelijke. De opdracht van UWV is juist om de persoonsgegevens te verwerken.**
- **Interne verstrekking van grote bestanden met persoonsgegevens uit analyseomgevingen geschiedt altijd via de divisie Gegevensdiensten.**

5.7. Gebruik van open bronnen (Google, social media, openbare registers)

5.7.1. Raadplegen van open bronnen

Op internet is veel informatie te vinden over personen. Via een zoekmachine zoals Google, het bekijken van (niet-afgeschermd) profielen op social media of door het raadplegen van openbare registers zoals het Kadaster en de Kamer van Koophandel kan je van alles te weten komen over een specifieke persoon. Hoewel deze informatie openbaar beschikbaar is gesteld, wordt deze informatie beschouwd als behorend tot het privé-domein. Deze openbare informatie over een persoon valt ook onder het begrip persoonsgegevens en het verzamelen en gebruik hiervan moet ook aan de eisen van de AVG voldoen.

Dit betekent dat deze informatie in het kader van de uitvoering van onze taken niet zomaar vrijelijk gebruikt mag worden, ondanks dat we dat in ons privéleven misschien wel gewend zijn. Het verschil zit er in dat we in ons privéleven dit over het algemeen doen in het kader van 'een zuiver persoonlijke of huisdoudelijke activiteit' doen en hierop is de AVG niet van toepassing⁴⁷. Voor het raadplegen van deze bronnen in het kader van onze taken op werk geldt deze uitzondering niet en is de AVG van toepassing. Het googlen van een klant of sollicitant is dus niet zomaar toegestaan.

Als uitgangspunt geldt dat het zoeken naar gegevens over een of meerdere specifieke personen op internet niet behoort tot de taken van UWV. Dit dient daarom achterwege te blijven. Er zijn drie situaties waarin op dit uitgangspunt een uitzondering kan worden gemaakt. Dat geldt voor:

⁴⁷ Artikel 2 lid 2 (c) AVG

- de controlerende taken die directie Handhaving heeft in het kader van voorkoming en bestrijding van fraude in overeenstemming met het *Protocol internetonderzoek Directie Handhaving UWV, laatst bijgewerkt op DWU op 15-5-2019*
- de onderzoekstaken van Bureau Integriteit in overeenstemming met het *Onderzoeksprotocol Bureau Integriteit UWV*, en
- in het kader van sollicitatieprocedures, maar alleen *met medeweten van de kandidaat* (conform de NVP-sollicitatiecode) en voor zover de informatie relevant is voor de functie. Dit moet in de vacaturetekst worden aangegeven.

In lijn met het voorgaande koopt UWV ook geen persoonsgegevens van derden om de eigen informatie of gebruikersprofielen te verrijken.

5.7.2. Gebruik social media door UWV

Daarnaast geldt dat UWV (Concerncommunicatie en K&S) zelf ook gebruik maakt van social media, zoals Twitter, Facebook en LinkedIn, om informatie van en over UWV te publiceren. Vanuit het perspectief van privacy moeten daarbij twee factoren in het oog worden gehouden.

- In de eerste plaats geldt dat UWV in beginsel geen berichten plaatst op social media waarin persoonsgegevens worden gedeeld.
- In de tweede plaats moet worden voorkomen dat klanten of derden (gevoelige) persoonsgegevens delen via het door UWV gebruikte platform. Zie ook paragraaf 7.4 inzake Veilig communiceren van persoonsgegevens.

UWV beleidskader

- **UWV maakt alleen in uitzonderlijke gevallen gebruik van persoonsgegevens die zijn verzameld uit open bronnen zoals social media en via zoekmachines op internet. Die organisatieonderdelen die hiervan gebruik kunnen maken, hebben hiervoor protocollen opgesteld die moeten zijn afgestemd met Juridische Zaken.**
- **Over het gebruik door UWV van eigen social media-accounts voor communicatie- en dienstverleningsdoeleinden wordt aanvullend beleid opgesteld dat in overeenstemming dient te zijn met de AVG en dit beleidskader en moet worden afgestemd met Juridische Zaken.**

5.8. Analyse, profilering en geautomatiseerde besluitvorming

UWV beschikt over zeer grote hoeveelheden persoonsgegevens. Deze zijn verzameld in het kader van de uitvoering van de wettelijke taken m.b.t. de rechtmatige verstrekking van uitkeringen, re-integratie en arbeidsbemiddeling en beoordelingen van claims/arbeidsvermogen. Daarnaast beschikt UWV over persoonsgegevens omdat de wet bepaalde organisaties verplicht deze aan UWV te verstrekken, bijvoorbeeld gegevens van werkgevers in verband met de loonaangifteketen. Ook worden data over het online-gedrag van klanten verzameld. In een tijd waarin data het nieuwe goud is, is UWV dan ook een goudmijn. UWV kan deze grote hoeveelheid persoonsgegevens gebruiken om bepaalde analyses op te verrichten. Analyses kunnen als doel hebben om terug te kijken naar een bepaalde ontwikkeling. Maar analyses kunnen ook als doel hebben om bepaalde (risico)modellen of klantprofielen op te stellen gericht op het voorspellen van bepaald gedrag (bijv. potentiële fraudeurs). Hierbij wordt vaak gebruik gemaakt van (complexe) algoritmen.

Zowel maatschappelijk als politiek bestaat veel aandacht voor de toepassing van algoritmen en kunstmatige intelligentie door de overheid. De Raad van Bestuur vindt het belangrijk dat de toepassing van algoritmen en kunstmatige intelligentie binnen UWV zorgvuldig, transparant en uitlegbaar gebeurt. Op diverse plekken in de organisatie worden momenteel complexe data-analysetoepassingen gebruikt waar een vorm van kunstmatige intelligentie deel vanuit maakt. Het gaat bijvoorbeeld om modellen (klantprofielen) die zijn ontwikkeld met behulp van algoritmen en die bedoeld zijn om klanten in te delen in bepaalde groepen om vervolgens de bejegening van die klant af te stemmen op de groep waarin die klant valt. Zonder een (toets)kader waarin naast de juridische aspecten ook aandacht is voor de ethische aspecten, brengt de toepassing hiervan de nodige risico's met zich mee.

In 2020 is daarom de 'commissie datagestuurd werken' opgericht om verschillende datatoepassingen binnen UWV te bespreken en te komen tot een set van uitgangspunten waar datatoepassingen binnen UWV aan moeten voldoen. Daarnaast zijn diverse werkgroepen opgericht om na te denken over de visie op datagedreven werken. Dit heeft eind 2020 onder andere geresulteerd in de stukken 'Visie op datagedreven UWV, kaderstelling' en 'Visie op datagedreven UWV, Strategische vraagstukken'. Zie hiervoor bijlage I.

Voor dit beleidskader is vooral van belang dat wanneer data-analyses en algoritmen worden toegepast op persoonsgegevens, deze verwerkingen moeten voldoen aan de eisen van de AVG. Belangrijk risico is dat de uitkomsten van deze nieuwe technologie niet goed uitlegbaar zijn. Wanneer deze gevolgen hebben voor de klant, moet UWV in staat zijn die uitkomst aan de klant (en eventueel aan een rechter) uit te leggen. Een ander belangrijk risico is dat de selectie van data die wordt gebruikt ertoe kan leiden dat bijv. het model dat met kunstmatige intelligentie tot stand is gekomen, discriminatoir is. Dit is vanzelfsprekend niet acceptabel voor UWV.

In deze paragraaf wordt op hoofdlijnen ingegaan op de voorwaarden die op grond van de AVG gelden voor data-analysetoepassingen waarbij persoonsgegevens worden gebruikt.

5.8.1. Analyses op basis van persoonsgegevens

Wat zegt de AVG?

Het analyseren van persoonsgegevens is een verwerking in de zin van de AVG en moet dus aan alle eisen van de AVG voldoen. Dit geldt ook wanneer analyses plaatsvinden op basis van gepseudonimiseerde persoonsgegevens. Alleen wanneer de persoonsgegevens *onomkeerbaar* zijn geanonimiseerd en op geen enkele wijze tot individuen zijn te herleiden, is de AVG niet van toepassing.
Overweging 26 AVG.

In een analyseomgeving zijn grote hoeveelheden persoonsgegevens samengebracht om te worden gebruikt voor het uitvoeren van analyses. Hoewel daarvoor niet primair bedoeld, worden de analyseomgevingen ook gebruikt voor productiedoeleinden (dit wordt ook wel omschreven als compensatie van bronsystemen, zie ook hierna). Dergelijke analyseomgevingen vormen een risico voor de privacy van de betrokkenen, wanneer de persoonsgegevens die daarin zijn opgenomen niet zijn geanonimiseerd (zie hierna). Niet alleen goede beveiliging van de analyseomgeving, maar ook toezicht op degene die daartoe toegang hebben en op de activiteiten die met de persoonsgegevens worden verricht is van groot belang.

Binnen UWV bestaan op dit moment bij diverse organisatieonderdelen verschillende analyseomgevingen waarin grote hoeveelheden persoonsgegevens worden bewaard. Dit heeft als risico dat er onvoldoende grip is op de analyseomgevingen en het toepassen van privacymaatregelen op deze omgevingen.

Eén uniform regime voor alle UWV analyseomgevingen

Om gecontroleerd gebruik van persoonsgegevens voor analysedoeleinden te waarborgen, dient als uitgangspunt te gelden dat alle analyseactiviteiten binnen UWV, ongeacht in welk organisatieonderdeel zij plaatsvinden, onder één uniform regime plaatsvinden dat door de divisie Gegevensdiensten wordt opgesteld. Dat uniforme regime houdt in dat duidelijke regels zijn vastgelegd over bijvoorbeeld de beveiliging van en de toegang tot de analyseomgeving, de toetsing van de werkzaamheden die daarbinnen mogen plaatsvinden en over het schonen van de analyseomgevingen. In december 2020 is hiertoe de 2.0 versie van het 'UWV Inrichtings- en toetsingskader voor big data-, data analyse omgevingen en datawarehouses' vastgesteld door de Raad van Bestuur (zie link in de bijlage). De verantwoordelijkheid voor het normenkader en de hierop gebaseerde monitorfunctie is belegd bij de directeur Gegevensdiensten.

Analyses op geanonimiseerde (persoons)gegevens

Omdat analyses per definitie worden uitgevoerd met gebruikmaking van grote hoeveelheden gegevens, geldt als uitgangspunt dat analyses plaatsvinden op basis van geanonimiseerde (persoons)gegevens. Dit volgt ook uit het beginsel van proportionaliteit/minimalisatie van gegevensverwerking. Voor veel analyses is het niet nodig om gegevens te gebruiken die te herleiden zijn tot op persoonsniveau. Het gaat bijvoorbeeld om het in kaart

brengen van trends en ontwikkelingen. Dit kan door een set gegevens te selecteren waaruit alle gegevens zijn verwijderd die, zelfstandig of in combinatie met elkaar, kunnen leiden naar de identiteit van het individu. Wanneer de gebruikte gegevens niet (meer) te herleiden zijn tot een individuele persoon, is er in principe geen risico voor de privacy van individuen. Zoals ook in paragraaf 2.1.2 is aangegeven vallen verwerkingen van onomkeerbaar geanonimiseerde persoonsgegevens niet onder de regels van de AVG. Voor het anonimiseren van persoonsgegevens is een *UWV Richtlijn Data Anonimisering en pseudonimisering* opgesteld (zie link in bijlage).

Analyses op gepseudonimiseerde persoonsgegevens

In sommige gevallen kan het nodig zijn om de uitkomsten van een analyse wél te kunnen herleiden tot persoonsniveau. Dit kan het geval zijn wanneer het noodzakelijk is de uitkomsten van de analyse te verifiëren en dit alleen mogelijk is door op individueel niveau een controle uit te voeren. Of wanneer de analyse er nu juist op is gericht om bepaalde personen te identificeren (bijv. hoog risico op fraude).

In dat geval kunnen analyses worden verricht op basis van gepseudonimiseerde persoonsgegevens. In dergelijke gevallen zal aan de volgende aspecten aandacht moeten worden besteed:

- Een motivatie waarom de analyse niet op onomkeerbaar geanonimiseerde persoonsgegevens kan worden uitgevoerd.
- Wie beheert de 'sleutel' waarmee de gepseudonimiseerde persoonsgegevens kunnen worden ontsleuteld zodat de betrokken individuele personen zichtbaar worden?
- Een duidelijke omschrijving van de gevallen waarin van de sleutel gebruik zal worden gemaakt.

Deze vragen zullen voorafgaand aan de verwerking beantwoord moeten worden, bijvoorbeeld in het kader van het GEB-proces.

In paragraaf 2.1.3 is aangegeven dat pseudonimisering een goede methode is om onnodige kennisneming van persoonsgegevens te voorkomen, maar dat ook gepseudonimiseerde persoonsgegevens onder de werking van de AVG vallen.

In de praktijk blijkt dat veel analyses plaatsvinden op niet-geanonimiseerde en niet-gepseudonimiseerde persoonsgegevens. Dat komt omdat voor de analyse gebruik wordt gemaakt van persoonsgegevens die in verschillende systemen en bronnen zijn opgeslagen. Omdat binnen UWV het BSN als hét koppelgegeven wordt gebruikt, worden de verschillende persoonsgegevens binnen een analyseomgeving aan elkaar gekoppeld door middel van het BSN. In dergelijke gevallen is geen sprake van geanonimiseerde gegevens noch van gepseudonimiseerde gegevens. Dergelijke analyses zullen daarom aan alle eisen van de AVG moeten voldoen.

Analyses en de privacybeginselen

Bij het uitvoeren van analyses – ook als sprake is van gepseudonimiseerde persoonsgegevens – zullen dus de beginselen van hoofdstuk 3 in acht moeten worden genomen. Denk hierbij aan de volgende vragen:

■ Is er een grondslag?

Ook voor het analyseren van persoonsgegevens moet een grondslag bestaan (zie hoofdstuk 4). In bepaalde gevallen is het uitvoeren van analyses in de wet (Wet SUWI) als taak aan UWV toebedeeld. Denk bijvoorbeeld aan het arbeidsmarktanalyse en bepaald onderzoek ten behoeve van het ministerie van SZW. Analyses worden ook uitgevoerd om bijvoorbeeld een (risico)model te ontwikkelen dat vervolgens in een proces zal worden ingezet. Ook in dat geval zal moeten worden nagegaan of de ontwikkeling en de toepassing van dat model noodzakelijk is ter uitvoering van de wettelijke taken van UWV. Die noodzaak moet goed worden gemotiveerd. Wanneer het uitvoeren van een analyse niet is terug te voeren op een van de wettelijke taken van UWV, moet er een andere grondslag zijn. In dat geval moet Juridische Zaken worden geconsulteerd. Is deze er niet of kan de noodzaak niet worden aangetoond, dan is het uitvoeren van een analyse op (gepseudonimiseerde) persoonsgegevens onrechtmatig.

■ Is voor de betrokkenen duidelijk dat hun gegevens ook worden verwerkt voor analysedoeleinden?

Het beginsel van transparantie geldt ook voor de verwerking van (gepseudonimiseerde) persoonsgegevens voor analysedoeleinden. Dit betekent dat voor de betrokkenen (degene van wie persoonsgegevens worden gebruikt voor analyses) duidelijk moet zijn dat hun gegevens (ook) voor deze doeleinden worden verwerkt. Dit kan door middel van de privacyverklaring.

- Is er doelbinding of is het gebruik van de gegevens verenigbaar met het oorspronkelijke doel?

De analyses die binnen UWV worden verricht worden in de meeste gevallen verricht op basis van persoonsgegevens die voor een ander doel zijn verkregen, bijvoorbeeld gegevens uit de polisadministratie of gegevens die zijn verkregen in het kader van de aanvraag van een uitkering. Wanneer analyses worden verricht op dergelijke gegevens zal moeten worden nagegaan of het doel van de analyse *verenigbaar* is met het doel waarvoor de gegevens zijn verzameld. Dit is een juridisch vraagstuk en vergt goede kennis van de AVG. Het dringende advies is daarom om de onderbouwing van de verenigbaarheid met behulp van de privacyjuristen van JZ te doen en deze vast te leggen in bijvoorbeeld een GEB.

In sommige gevallen worden gegevens wél specifiek verzameld met het doel daarmee analyses te verrichten. Dit wordt bijvoorbeeld gedaan door K&S: gegevens over het klikgedrag van klanten die de website van UWV bezoeken worden bijvoorbeeld verzameld om de website te optimaliseren. Overigens is het voor het optimaliseren van de website niet nodig om analyses uit te voeren op niet-geanonimiseerde persoonsgegevens. Voor dergelijke analyses kunnen de anonieme gegevens worden verzameld en geanalyseerd.

Wanneer een analyse wordt verricht op basis van (gepseudonimiseerde) persoonsgegevens, moet vooraf duidelijk zijn welk doel met de analyse wordt gediend. Dit moet zijn vastgelegd.

- Worden niet méér persoonsgegevens gebruikt dan noodzakelijk voor het doel en hebben niet méér personen toegang tot de analyseomgeving dan noodzakelijk voor het doel?

Zoals hierboven al is aangegeven, leidt het beginsel van minimale gegevensverwerking ertoe dat als uitgangspunt geldt dat analyses op onomkeerbaar geanonimiseerde persoonsgegevens worden uitgevoerd. Voor zover persoonsgegevens worden verzameld of geselecteerd specifiek voor analysedoeleinden, wordt ook verzekerd dat uitsluitend die gegevens worden verzameld die noodzakelijk zijn om de desbetreffende analyse uit te voeren en niet méér.

Dit beginsel houdt ook in dat steeds kritisch moet worden gekeken wie toegang krijgt tot de analyseomgeving. UWV moet waarborgen dat dit uitsluitend die personen zijn voor wie toegang ook noodzakelijk is voor de taak die zij met betrekking tot de analyse verrichten en dat de toegang beperkt is tot de duur van deze taak. Dit moet zijn vastgelegd.

- Zijn de gegevens die voor de analyse worden gebruikt correct?

Ook bij het uitvoeren van analyses op basis van persoonsgegevens moeten alleen gegevens die correct en actueel zijn worden gebruikt. Waar persoonsgegevens gebruikt worden voor het ontwikkelen van een voorschrijvend of voorspellend model, geldt deze eis nog sterker en is de kwaliteit van de data van groot belang. Wanneer de data verouderd is en ongelijksoortige data gelijksoortig wordt behandeld, kan dit leiden tot onbetrouwbare uitkomsten. Dit moet voorkomen worden, zeker wanneer die uitkomsten gevolgen hebben voor de individuele klant.

Voordat een analyse wordt verricht moet de correctheid van de data worden gecontroleerd. De waarborgen die zijn getroffen om de correctheid van de data te verzekeren moeten zijn vastgelegd.

- Welke bewaartermijnen worden gehanteerd?

Uitgangspunt van de AVG is dat persoonsgegevens niet langer mogen worden bewaard dan nodig is voor het doel waarvoor ze worden verwerkt. Ook in het kader van analyseomgevingen moet daarom zijn gewaarborgd dat de gegevens niet langer worden bewaard dan is toegestaan. Zie voor de geldende bewaartermijnen het door Data Office in afstemming met DIV opgestelde beleidsdocument *Bewaartermijnen DWH-omgeving, versie 2.6* (link in bijlage).

- Is de analyseomgeving adequaat beveiligd?

De omgeving waarbinnen persoonsgegevens worden geanalyseerd moet adequaat beveiligd zijn. Dat geldt in het bijzonder omdat een analyseomgeving doorgaans een zeer grote hoeveelheid persoonsgegevens bevat. Een passend beveiligingsniveau is gerelateerd aan de classificatie van de gegevens en de manier waarop de gegevens worden verwerkt. Zie voor het onderwerp beveiliging hoofdstuk 7.

Centrale verstrekking van persoonsgegevens uit analyseomgevingen voor productiedoeleinden

Op dit moment komt het voor dat aan de afdelingen die toegang hebben tot analyseomgevingen verzoeken worden gedaan om een verzameling van persoonsgegevens te verstrekken die voor productiedoeleinden wordt gebruikt. Deze verzoeken worden gedaan door organisatieonderdelen die zelf niet in staat zijn om de benodigde verzameling van gegevens op te hoesten omdat de doelsystemen daartoe niet in staat zijn.

Zolang er onvolkomenheden in de doelsystemen zijn, is er op zich geen bezwaar om aan dergelijke verzoeken gehoor te geven, maar ook hiervoor geldt dat controle hierover noodzakelijk is, o.a. om onnodige data-redundantie tegen te gaan. Daarom geldt dat dergelijke verzoeken centraal moeten worden afgehandeld. Dit betekent dat dergelijke verzoeken tot de divisie Gegevensdiensten worden gericht die tevens kan toetsen of de verstrekking van de gevraagde gegevens in het concrete geval rechtmatig is. De organisatieonderdelen die zelf beschikken over een analyseomgeving, doen dergelijke verzoeken dan dus niet meer zelf af en kunnen dat ook niet wanneer die omgevingen alleen nog bestaan uit onomkeerbaar geanonimiseerde gegevens. Zij sturen de collega die hierom verzoekt door naar de divisie Gegevensdiensten (zie ook paragraaf 5.6).

Bij de verstrekking zullen ook afspraken moeten worden gemaakt over de wijze waarop de verstrekte gegevens worden bewaard, wie er toegang toe hebben en wanneer ze moeten worden vernietigd. Bij dit laatste punt moet rekening worden gehouden met de vereisten voor de vernietigingsprocedure die voortvloeien uit de archiefwetgeving. De afdeling DIV is verantwoordelijk voor de inrichting van de vernietigingsprocedure binnen UWV en kan het desbetreffende organisatieonderdeel adviseren.

UWV beleidskader

- **Uitgangspunt is dat één uniform regime tot stand wordt gebracht waaraan alle analyseomgevingen binnen UWV moeten voldoen. De divisie Gegevensdiensten stelt dit regime op. Het uniforme regime bestaat uit duidelijke regels over de beveiliging en toegang tot analyseomgevingen, toetsing van de werkzaamheden die daarbinnen worden verricht en over het verwijderen van gegevens uit de analyseomgevingen op grond van de vereisten uit de archiefwetgeving.**
- **Als uitgangspunt geldt dat analyses worden uitgevoerd op onomkeerbaar geanonimiseerde persoonsgegevens. Als het nodig is om de uitkomsten van de analyses terug te leiden tot persoonsniveau, kunnen analyses worden verricht op gepseudonimiseerde persoonsgegevens. Dit moet gemotiveerd worden aangegeven. Voorafgaand aan dergelijke verwerkingen wordt een GEB uitgevoerd. Daarin wordt onder andere ingegaan op de vraag wie de 'sleutel' beheert en in welke gevallen deze mag worden gebruikt.**
- **Alleen in uitzonderingsgevallen worden analyses uitgevoerd op niet-gepseudonimiseerde persoonsgegevens. De FG wordt hiervan door middel van een GEB vooraf in kennis gesteld en adviseert hierover.**
- **Het gebruik van en de verstrekking van persoonsgegevens uit analyseomgevingen voor productiedoeleinden geschiedt centraal door de divisie Gegevensdiensten. Indien een verzoek tot verstrekking van gegevens bij een ander organisatieonderdeel binnenkomt, wordt de verzoeker doorverwezen naar Gegevensdiensten.**

5.8.2. Profileren van personen op basis van persoonsgegevens (het ontwikkelen en gebruiken van klant- en risicoprofielen)

Wat zegt de AVG?

Van profilering van personen is sprake wanneer op geautomatiseerde wijze persoonsgegevens worden verzameld, geanalyseerd en/of gecombineerd met als doel mensen op basis van generieke kenmerken in te delen in bepaalde categorieën (bijv. klantprofielen). Het profileren van personen is een verwerking van persoonsgegevens die onder de AVG valt en dus aan alle eisen van de AVG moet voldoen. Profileren als

zodanig is niet verboden, maar wel in combinatie met geautomatiseerde besluitvorming met rechtsgevolgen of andere aanmerkelijke gevolgen voor de betrokkene.

Artikel 4 (4) AVG en Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679 van de Groep Gegevensbescherming Artikel 29

Wanneer analyses en andere geautomatiseerde verwerkingen van persoonsgegevens erop zijn gericht personen op basis van generieke kenmerken in bepaalde (risico)groepen in te delen, is sprake van profilering. Het kan bijvoorbeeld gaan om het indelen van personen in een groep met bepaalde voorkeuren, met een bepaalde mate van betrouwbaarheid of een bepaald bestedingsvermogen.

Van profilering als bedoeld in de (U)AVG is sprake als de volgende drie elementen aanwezig zijn:

- het gaat om een *geautomatiseerde* vorm van verwerking;
- het gaat om de verwerking van *persoonsgegevens*; en
- het doel van de profilering is om personen op basis van *generieke kenmerken* in groepen in te delen.

Het profileren van personen op basis van generieke kenmerken is op zichzelf niet verboden onder de AVG.

Geautomatiseerde besluitvorming met rechtsgevolgen of andere aanmerkelijke gevolgen voor de betrokkene op basis van profilering is echter niet toegestaan (zie paragraaf 5.8.3).⁴⁸ Dit betekent dat wanneer in een bepaald proces gebruik wordt gemaakt van klant- of risicoprofielen het op zichzelf is toegestaan dat klanten op basis van bepaalde kenmerken geautomatiseerd in een bepaalde categorie worden ingedeeld. Deze indeling mag echter niet direct leiden tot een bepaald gevolg voor de klant. Altijd moet verzekerd zijn dat beslissingen met gevolgen voor de klant door een medewerker mede op basis van andere gegevens en factoren worden genomen. Dit noemen we ook wel 'betekenisvolle menselijke tussenkomst'.

In de dienstverlening van UWV wordt gebruik gemaakt van profilering van klanten. Voorbeelden hiervan zijn:

- het geautomatiseerd bepalen van persoonlijke voorkeuren van klanten voor een bepaalde vorm van dienstverlening;
- het geautomatiseerd indelen van klanten in een groep werkzoekenden die extra begeleiding nodig heeft;
- het geautomatiseerd indelen van klanten in een groep met een hoog risico op fraude.

Omdat bij profilering van personen het risico bestaat dat een individu in een bepaalde categorie (groep) van klanten belandt, terwijl het generieke kenmerk op dat individu niet van toepassing is, kan dit ten onrechte nadelige gevolgen voor de betrokkene hebben. Daarom moet bij een voorgenomen toepassing van profilering van klanten, een zeer zorgvuldige afweging worden gemaakt van de risico's. Van te voren moet bijvoorbeeld inzicht bestaan in de generieke kenmerken die ertoe leiden dat een betrokkene in een bepaalde categorie wordt ingedeeld en de gevolgen voor de betrokkene die daaraan zijn verbonden. Waarom is voor een bepaalde set criteria (generieke kenmerken) gekozen? Wat betekent het concreet als een klant in een bepaalde groep wordt ingedeeld? Wanneer de profilering weliswaar niet direct gekoppeld is aan geautomatiseerde besluitvorming, maar wel voorsorteert op menselijke besluitvorming, zal ook moeten worden stilgestaan bij de vraag hoe die menselijke tussenkomst betekenisvol kan zijn zodat het hierboven omschreven risico (generiek kenmerk wordt de klant ten onrechte tegengeworpen) wordt voorkomen.

Deze vragen en aspecten dienen goed te worden vastgelegd en gearchiveerd. Het is van belang dat UWV kan aantonen welke criteria bij profilering zijn gebruikt, waarom voor die criteria is gekozen en hoe wordt voorkomen dat klanten ten onrechte hiervan negatieve gevolgen ondervinden. Deze informatie moet daarom onderdeel vormen van een GEB of een protocol. Voor organisatieonderdelen die veelvuldig gebruik maken van profilering (bijvoorbeeld de directie Handhaving), ligt het in de rede hiervoor een protocol op te stellen waarin de relevante aspecten en vragen worden uitgewerkt.

UWV beleidskader

- **UWV maakt in bepaalde processen gebruik van profilering (het geautomatiseerd indelen van personen in verschillende groepen die aan bepaalde generieke kenmerken voldoen). Dit wordt echter nooit gecombineerd met geautomatiseerde besluitvorming.**

⁴⁸ Artikel 40 UAVG

- **Wanneer het voornemen bestaat om gebruik te maken van profilering, moeten de daaraan verbonden risico's en de wijze waarop deze risico's worden gemitigeerd vooraf in kaart zijn gebracht (GEB) of een protocol dat voor advies aan de FG en Juridische Zaken is voorgelegd.**
- **Er wordt gedocumenteerd welke generieke kenmerken/indicatoren bepalend zijn voor de indelingen in een categorie of groep, waarom voor deze kenmerken is gekozen en hoe wordt voorkomen dat klanten ten onrechte negatieve gevolgen ondervinden van de profilering. Deze informatie wordt gearhiveerd.**

5.8.3. Geautomatiseerde besluitvorming met rechtsgevolgen of andere aanmerkelijke gevolgen voor de betrokkene

Wat zegt de AVG?

Op grond van de AVG is het in principe verboden om volledig geautomatiseerd besluiten te nemen wanneer die besluiten rechtsgevolgen voor de betrokkene hebben of de betrokkene in aanmerkelijke mate treffen. Dit verbod geldt echter niet als er een wettelijke uitzondering is. In de UAVG zijn uitzonderingen op dit verbod opgenomen voor overheidsorganisaties, zoals UWV. Belangrijke voorwaarde is dat de geautomatiseerde besluitvorming noodzakelijk is voor de uitvoering van de publieke taak van UWV en deze verwerking plaatsvindt op basis van strikt individuele kenmerken en niet op basis van profilering.

Artikel 13 lid 2 (f) en artikel 22 AVG, artikel 40 UAVG, zie ook [Guidelines on individual automated decision-making and profiling van de WP29](#)

Op grond van de AVG is het organisaties in beginsel niet toegestaan volledig geautomatiseerd besluiten te nemen die voor de betrokkene rechtgevolgen hebben of die de betrokkene in aanmerkelijke mate raken. Dit wordt ook wel omschreven als het 'recht op menselijke tussenkomst'. In principe heeft iedere burger recht op een menselijke blik, wanneer besluiten over hem worden genomen die rechtsgevolgen voor hem hebben of hem anderszins in aanmerkelijke mate treffen.

Artikel 40 UAVG bevat een uitzondering op het verbod op geautomatiseerde besluitvorming die voor de betrokkene rechtgevolgen heeft of die de betrokkene in aanmerkelijke mate treft. Op grond van die uitzondering mogen overheidsorganisaties gebruik maken van geautomatiseerde individuele besluitvorming met rechtsgevolgen of andere aanmerkelijke gevolgen, wanneer dit noodzakelijk is voor de uitvoering van de wettelijke taken van algemeen belang. Voorwaarden die hierbij gelden zijn dat:

- a. de geautomatiseerde besluitvorming niet gebaseerd is op profilering (zie paragraaf 5.8.2); en
- b. de betrokkene, naast de informatie die hem sowieso over de verwerking moet worden verstrekt (zie paragraaf 8.1), ook vooraf wordt geïnformeerd over:
 - het feit dat een besluit genomen wordt op basis van een geautomatiseerd proces; en
 - de daaraan ten grondslag liggende logica. Dit moet op een voor de betrokkene begrijpelijke manier worden gedaan. Deze informatie zou in de privacyverklaring kunnen worden opgenomen.

Om aan deze eisen te voldoen, is het van belang dat het organisatieonderdeel dat gebruik maakt of wil maken van geautomatiseerde besluitvorming met rechtsgevolgen of andere aanmerkelijke gevolgen voor de betrokkene een duidelijk verantwoordingsdocument heeft waarin de logica (een uitleg van de werking van het algoritme/de beslisregels) die wordt gebruikt duidelijk staat uitgelegd. Ook moet in het register van verwerkingen (paragraaf 8.2) expliciet worden vermeld bij welke verwerkingen sprake is van geautomatiseerde besluitvorming.

Op grond van deze uitzondering mag UWV in zijn werkprocessen gebruik maken van geautomatiseerde besluitvorming die voor de betrokkene rechtgevolgen heeft of die de betrokkene in aanmerkelijke mate raakt. Hierbij gelden de volgende spelregels:

- het gaat om geobjectiveerde besluiten gebaseerd op in wet- en regelgeving vastgestelde criteria;
- het gaat om besluiten waarin UWV geen eigen beoordelingsruimte heeft (dit worden ook wel 'gebonden' besluiten of beschikkingen genoemd: het bestuursorgaan heeft geen eigen beleidsruimte, de beslissing vloeit rechtstreeks voort uit toepassing van wettelijke regels);

- het gaat om besluitvorming op basis van strikt individuele kenmerken; er is dus geen sprake van profilering zoals omschreven in de UAVG.

Een belangrijk proces waarin nu geautomatiseerde besluitvorming wordt toegepast is de toekenning van de WW-uitkering via het straight-through-proces. In dit proces wordt recht, hoogte en duur geheel automatisch vastgesteld. Geautomatiseerde besluitvorming is hier toegestaan omdat het besluit is gebaseerd op gebonden bevoegdheden op basis van objectieve, in wettelijke regelingen vastgelegde kenmerken die worden toegepast op strikt individuele kenmerken betreffende het specifieke individu. In het geval van de WW-uitkering, zijn de in de wet vastgelegde kenmerken de criteria die gelden voor het vaststellen van recht, hoogte en duur van de WW-uitkering. Deze zijn vastgelegd in de Werkloosheidswet en daarmee verband houdende regelgeving. Die criteria laten geen beoordelingsruimte voor de medewerkers van UWV. Waar gesproken wordt over de individuele kenmerken van het specifieke individu gaat het om de specifieke situatie van de individuele klant, zoals de hoogte van zijn laatstgenoten inkomen en zijn arbeidsduur.

Ook de automatische verwerking van de inkomensopgaven van uitkeringsgerechtigden (IKO) geschiedt volledig geautomatiseerd en is een vorm van geautomatiseerde besluitvorming met rechtsgevolgen voor de betrokkene. De uitkeringsgerechtigde geeft iedere maand (digitaal) aan UWV door welke inkomsten hij of zij heeft die maand heeft genoten. Deze inkomensopgave wordt geautomatiseerd verwerkt en leidt vervolgens automatisch tot een aangepast bedrag van de uitkering waarin de genoten inkomsten zijn verrekend. De aangepaste hoogte van de uitkering is beslissing met rechtsgevolgen voor de klant.

Het verschil tussen geautomatiseerde besluitvorming op basis van individuele kenmerken (toegestaan) en geautomatiseerde besluitvorming op basis van profilering (niet toegestaan), is dat de besluitvorming in het eerste geval wordt gebaseerd op een aantal vooraf en objectief vastgestelde variabelen die in een directe relatie staan tot de betrokkene (denk aan hoogte inkomen, duur arbeidsrelatie), terwijl de besluitvorming op basis van profilering wordt gebaseerd op de uitkomst van een proces waarin (persoons)gegevens worden verzameld en vervolgens geanalyseerd en/of gecombineerd met als doel mensen in te delen in bepaalde categorieën (profielen). Waar in het eerste geval de *individuele kenmerken* van de betrokken persoon beslissend zijn, zijn dat in het tweede geval de *generieke kenmerken* van de gehele groep personen die tot een bepaalde categorie behoren. Dit laatste brengt het risico met zich mee dat een besluit over de betrokkene wordt genomen op basis van een generiek kenmerk van de groep, terwijl dat kenmerk op hem niet van toepassing is.⁴⁹

Zou UWV in een proces gebruik willen maken van geautomatiseerde besluitvorming met rechtsgevolgen of andere aanmerkelijke gevolgen voor de betrokkene die wel is gebaseerd op profilering van personen, dan is hiervoor een expliciete *wettelijke* bepaling nodig.

Omdat UWV een bestuursorgaan is, moeten de besluiten van UWV, ook indien deze op geautomatiseerde wijze tot stand zijn gekomen, voldoen aan de eisen van de Awb (waaronder de algemene beginselen van behoorlijk bestuur). Hieruit volgt ook dat de besluiten vatbaar zijn voor bezwaar en beroep, waardoor voldaan wordt aan het vereiste van de UAVG dat passende maatregelen zijn genomen om de rechten van de betrokkene te beschermen.⁵⁰

UWV beleidskader

- **UWV maakt in bepaalde processen gebruik van geautomatiseerde individuele besluitvorming met rechtsgevolgen voor de betrokkene.**
- **Dit beperkt zich tot processen waarin de besluitvorming geen beoordelingsvrijheid toestaat en het besluit genomen wordt op basis van in de wet vastgelegde criteria die worden toegepast op strikt individuele kenmerken. Onder deze voorwaarden is er geen sprake van profilering.**

⁴⁹ Zie nota n.a.v. verslag bij wetsvoorstel UAVG, Kamerstukken II 2017/18, 34 851, nr. 7, p. 72.

⁵⁰ Artikel 40 lid 2 UAVG.

- **In het register van verwerkingen wordt aangegeven bij welke verwerking gebruik wordt gemaakt van geautomatiseerde besluitvorming.**
- **Betrokkenen worden voorafgaand aan de verwerking geïnformeerd over het feit dat gebruik wordt gemaakt van geautomatiseerde besluitvorming en in begrijpelijke woorden welke logica daarbij wordt gehanteerd.**
- **Door de proceseigenaar wordt in detail gedocumenteerd volgens welke logica het geautomatiseerde besluit tot stand komt.**

6. Bewaren en vernietigen van persoonsgegevens

Wat zegt de AVG?

Uitgangspunt van de AVG is dat persoonsgegevens niet langer mogen worden bewaard dan noodzakelijk is voor het doel waarvoor ze worden verwerkt, tenzij een specifieke wet verplicht de persoonsgegevens langer te bewaren. De Archiefwet is zo'n wet die verplicht tot langer bewaren. Dit betekent dat na het afsluiten van een zaak of dossier, de persoonsgegevens die UWV heeft verwerkt - ongeacht of ze op papier of digitaal zijn vastgelegd - worden gearchiveerd en gedurende een vastgestelde termijn worden bewaard. Daarna worden ze vernietigd of overgebracht naar het Nationaal Archief.

Artikel 5 lid 1 (e) en artikel 89 AVG, Archiefwet, Regeling archiefbeheer UWV, Selectielijst UWV, Data life cycle management

Hoofregel van de AVG is dat persoonsgegevens moeten worden vernietigd als ze niet meer nodig zijn voor het doel waarvoor ze worden verwerkt. Echter, UWV is een overheidsorganisatie en daarom geldt voor UWV de Archiefwet. Op basis van de Archiefwet moeten de papieren, gedigitaliseerde en digitale archiefbescheiden, ook als deze persoonsgegevens bevatten, na het afsluiten van een zaak of dossier nog een aantal jaren worden bewaard (gearchiveerd). Maar ook andere wetten schrijven voor bepaalde gegevens langere bewaartermijnen voor dan de AVG.⁵¹ Hoe lang de gegevens moeten worden bewaard, hangt af van het proces waarin de gegevens zijn gebruikt en de waarde van de informatie. In de zogenaamde selectielijst van UWV⁵² zijn de bewaartermijnen vastgelegd en wordt beschreven hoe de bewaartermijnen moeten worden toegepast. Deze bewaartermijnen beginnen te lopen vanaf het moment dat een zaak is afgesloten. Als de bewaartermijn is verstreken, moeten de gegevens worden vernietigd, tenzij zij - in uitzonderlijk gevallen - in aanmerking komen voor overbrenging naar het Nationaal Archief.

In sommige gevallen kan het voorkomen dat voor bepaalde documenten verschillende bewaartermijnen gelden omdat het document onderdeel uitmaakt van meerdere processen. Voorbeeld hiervan is een beschikking die is afgegeven voor een uitkering, maar tevens kan worden gebruikt in een re-integratietraject. Een dergelijk document maakt in dat geval onderdeel uit van twee dossiers met ieder zijn eigen bewaartermijn. Is de bewaartermijn van het document in het ene dossier afgelopen, dan wordt het document alleen nog bewaard ten behoeve van de archivering van het andere dossier.

Eén dossier kan ook documenten bevatten met verschillende bewaartermijnen, bijvoorbeeld medische documenten kennen een bewaartermijn van 10 jaar terwijl claimdocumenten een bewaartermijn kennen van 5 jaar. Nadat een dossier is afgesloten gaan al deze bewaartermijnen tegelijk lopen en worden claimdocumenten 5 jaar na afsluiting van het dossier vernietigd, terwijl medische documenten 10 jaar na afsluiting van het dossier worden vernietigd.

De Archiefwet is van toepassing op archiefbescheiden, dat wil zeggen op papieren, gedigitaliseerde of digitale documenten die door UWV zijn ontvangen of door UWV zelf zijn opgesteld bij de uitvoering van zijn wettelijke taken.⁵³ Denk hierbij aan brieven, e-mails, beschikkingen, vorderingen, rapporten, schriftelijke beoordelingen en dergelijke. Ook de gegevens die zijn opgenomen in (doel)systemen en procesapplicaties voor de uitvoering van de wettelijke taken vallen onder de archiefwetgeving. Aanwijzingen voor het bewaren en vernietigen van gegevens in doelsystemen en procesapplicaties zijn opgenomen in het door Data Office opgestelde document *Data Lifecycle Management bij UWV* (zie bijlage).

Op het moment dat de (persoons)gegevens niet langer noodzakelijk zijn voor het doel waarvoor ze worden verwerkt (een zaak of dossier is afgesloten en een eventueel ingesteld bezwaar of beroep is afgehandeld), is het voor de medewerkers niet langer noodzakelijk om toegang te hebben tot de desbetreffende gegevens. Hun werkzaamheden met betrekking tot die gegevens zijn immers afgerond. De Regeling archiefbeheer UWV bepaalt

⁵¹ Voorbeeld is fiscale wetgeving die verplicht bepaalde gegevens langer te bewaren.

⁵² Selectielijst Uitvoeringsinstituut werknemersverzekeringen (UWV) vanaf 2014 houdende het besluit inzake bewaartermijnen van archiefdocumenten voor het Uitvoeringsinstituut werknemersverzekeringen (Staatscourant 2017, nr. 9044).

⁵³ Artikel 1 onder c van de Regeling archiefbeheer UWV.

dan ook dat raadpleging van de documenten en gegevens in een bepaalde zaak, na afronding van die zaak, alleen is toegestaan na toestemming van de verantwoordelijke voor het archief. Bij UWV vervult hoofd DIV de functie van archivaris.

De toestemming van hoofd DIV voor raadpleging van documenten in EA zal via een vooraf opgesteld plan worden gegeven. Uit dit opgestelde plan dient te blijken welke taken aan welke functionarissen zijn toebedeeld en welke informatie noodzakelijk is voor de uitvoer van die taak ten behoeve van die persoon op dat moment. Slechts in uitzonderlijke gevallen moet op het moment dat toegang nodig is nog worden onderzocht of deze toestemming kan worden verleend.⁵⁴

Voor de papieren dossiers is dit vrij eenvoudig te realiseren. De papieren dossiers worden na het afsluiten van een zaak uiteindelijk overgebracht naar het archief van UWV. Het beheer van dit papieren archief heeft UWV uitbesteed aan een extern bedrijf. Voor zover de papieren dossiers nog niet zijn overgebracht naar de centrale opslag, kan raadpleging ervan eenvoudig worden voorkomen door de dossiers in een afgesloten kast te bewaren totdat zij naar de centrale opslag worden overgebracht.

Voor digitale gegevens ligt dit ingewikkelder. De gegevens die voor archivering in aanmerking komen, zijn immers verspreid over verschillende doelsystemen en het Elektronisch Archief (EA). Daarnaast kunnen ook op andere plaatsen gegevens zijn opgeslagen die voor archivering in aanmerking komen (denk aan de opslag van ongestructureerde informatie⁵⁵). Voor de doelsystemen en het EA geldt dat deze systemen zowel worden gebruikt om gegevens en documenten in op te slaan ten behoeve van gebruik in het primaire proces als voor de archivering van die gegevens en documenten na het afsluiten van een zaak. Om aan de AVG en de Archiefwet te voldoen, is het daarom van belang dat in de verschillende doelsystemen en in EA een onderscheid wordt aangebracht tussen de gegevens die noodzakelijk zijn voor het primaire proces en – als de zaak eenmaal is afgehandeld – de gegevens die voor archivering in aanmerking komen. Dit onderscheid is in de eerste plaats van belang gelet op de beperkte toegang die geldt voor gearhiveerde gegevens (zie hierboven). In de tweede plaats is het van belang om het moment van het afhandelen van de zaak te markeren, omdat de bewaartermijnen van de archiefwetgeving vanaf dat moment beginnen te lopen. Alleen wanneer dat moment in de systemen goed is gemarkeerd, zal immers kunnen worden vastgesteld op welk moment de gegevens moeten worden vernietigd. Dit is typisch een aspect van *privacy by design* en *archivering by design* dat bij de ontwikkeling van nieuwe systemen moet worden meegenomen.

Aandachtspunt hierbij is het volgende. Om onbevoegde kennisneming van persoonsgegevens via eventuele kopieën te voorkomen, geldt binnen UWV het uitgangspunt dat dergelijke kopieën uiterlijk worden vernietigd wanneer de zaak of het dossier is afgerond. Alleen het origineel blijft dan in het archief bewaard.

Tenslotte geldt dat de persoonsgegevens mogen worden bewaard in het archief van UWV maar na afloop van de bewaartermijn moeten worden vernietigd of bij uitzondering op termijn worden overgedragen aan het Nationaal Archief als onderdeel van cultureel erfgoed en/of voor historisch onderzoek.

Een begrip dat verbonden is met de vraag wanneer een gegeven vernietigd mag worden is het begrip 'zaak'. Hieronder wordt een samenhangende hoeveelheid werk verstaan ten behoeve van de dienstverlening aan een externe klant. De zaak heeft een gedefinieerde aanleiding en een gedefinieerd eindresultaat, en de kwaliteit en doorlooptijd ervan moet worden bewaakt. Het zaakbegrip kan een sleutel vormen om voor clusters van gegevens te kunnen bepalen wanneer de bewaartermijn start (namelijk als de zaak wordt beëindigd) en wanneer de gegevens moeten worden vernietigd. Meer informatie met betrekking tot zaakgericht werken is te vinden in het kennisportaal 'Werken met Zaken': <https://digitalewerkplek.sharepoint.uwv.nl/uwv/programmas-en-projecten/Paginas/KennisportaalWerkenmetZaken.aspx>

UWV beleidskader

- **FB DIV en Data Office stellen beleid op over het bewaren, archiveren en vernietigen van persoonsgegevens in het EA en in de andere (doel)systemen van UWV. Hierbij is het opstellen van**

⁵⁴ Artikel 4 lid 6 Regeling archiefbeheer UWV

⁵⁵ Onder ongestructureerde informatie wordt in dit verband verstaan informatie onderdeel dient uit te maken van het dossier, maar niet in een doelsysteem of applicatie kan worden opgeslagen.

archiefbeleid voorbehouden aan FB DIV. Alle organisatieonderdelen moeten aan de uitvoering van dat beleid meewerken.

- In de processen van UWV wordt een onderscheid gemaakt tussen het bewaren van persoonsgegevens (zolang een zaak nog niet is afgehandeld) en het archiveren van persoonsgegevens (nadat een zaak is afgehandeld).
- De bewaartermijnen die zijn opgenomen in de selectielijst van UWV gaan lopen vanaf het moment dat een zaak is afgerond.
- Indien een document in verschillende processen wordt gebruikt, kunnen voor dat document verschillende bewaartermijnen gelden. Raadpleeg hiervoor de selectielijst van UWV.
- In principe is de toegang tot (persoons)gegevens die zijn gearcheveerd, beperkt tot degene die verantwoordelijk is voor het archief (hoofd FB DIV). Alleen na toestemming van de voor het archief verantwoordelijke, kan toegang tot de gearcheveerde gegevens worden verkregen.
- Om onbevoegde kennisneming van gearcheveerde gegevens en documenten te voorkomen, moeten uiterlijk op het moment dat een zaak is afgerond eventuele kopieën van die gegevens en documenten die op andere plaatsen zijn opgeslagen worden vernietigd.
- Door middel van *privacy by design* en *archivering by design* wordt in het voortbrengingsproces UWV tegemoet gekomen aan deze vereisten vanuit de AVG en archiefwetgeving.

7. Beveiliging van persoonsgegevens

Wat zegt de AVG?

Iedere organisatie die persoonsgegevens verwerkt moet passende technische en organisatorische maatregelen nemen om een op het risico afgestemd beveiligingsniveau te waarborgen. Bij de bepaling welke maatregelen passend zijn, wordt rekening gehouden met de stand van de techniek, de uitvoeringskosten en de aard, omvang, context en doelen van de verwerking. Wat betreft de mogelijke risico's wordt gekeken naar de waarschijnlijkheid (kans) en ernst (impact) van de risico's voor de rechten en vrijheden van de betrokkene. *Artikel 5 lid 1 (f) en artikel 32 AVG, BIR UWV, SUWI normenkader*

Een heel belangrijk aspect van de bescherming van persoonsgegevens is dat de persoonsgegevens adequaat zijn beveiligd. Hiervoor moeten zowel technische als organisatorische maatregelen worden getroffen.

Op het terrein van informatiebeveiliging heeft UWV zich sinds 1 januari 2020 te houden aan de Baseline Informatiebeveiliging Overheid (BIO). UWV volgt deze normenkaders om invulling te geven aan de vereisten van de AVG op het gebied van beveiligingsmaatregelen (paragraaf 7.1). De BIO beperkt zich echter niet tot het beveiligen van persoonsgegevens en de bescherming van privacy, maar is ook van toepassing op andere gevoelige informatie die geen persoonsgegevens bevat. Denk hierbij bijvoorbeeld aan informatie over een aanbestedingstraject.

Ook autorisatiebeheer is een belangrijk element om onbevoegde kennisneming van (gevoelige) persoonsgegevens te voorkomen. Daarnaast zijn organisatorische maatregelen om de toegang tot fysieke dossier te reguleren hierbij van belang. (paragraaf 7.2)

Tenslotte communiceert UWV heel veel met de buitenwereld. Met klanten en met partners, met leveranciers en met medewerkers. Gelet op de aard van de werkzaamheden van UWV gaat het hierbij veelal om communicatie van persoonsgegevens. Vanzelfsprekend moet dit op een veilige manier gebeuren. Hierop wordt in paragraaf 7.3 ingegaan.

7.1. De Baseline Informatiebeveiliging Overheid (BIO)

De Baseline Informatiebeveiliging Overheid (BIO) beoogt de beveiliging van informatie(systemen) bij alle bestuurslagen en bestuursorganen van de overheid te bevorderen, zodat alle onderdelen erop kunnen vertrouwen dat onderling uitgewisselde gegevens, in lijn met wet- en regelgeving, passend beveiligd zijn. Het doel van de BIO is continuïteit in de bedrijfsprocessen door waarborgen van juiste en tijdige informatie.

De BIO is een normenkader voor informatiebeveiliging (IB) en geeft het basisniveau voor informatiebeveiliging waar alle overheidspartijen aan moeten voldoen. De BIO is allereerst een gemeenschappelijk normenkader voor de beveiliging van de informatie(systemen) van de overheid. Daarnaast concretiseert de BIO een aantal normen tot verplichte overheidsmaatregelen. Het is gebaseerd op de actuele, internationale standaarden voor informatiebeveiliging, de ISO 27001 en 27002. Door dit eenduidige normenkader binnen de overheid, wordt een stevige basis gelegd voor de verdere optimalisering van informatiebeveiliging binnen de gehele overheid en ontstaat een gemeenschappelijke taal die bijdraagt aan veilige samenwerking in ketens binnen de overheid. Uitgangspunt van de BIO bij implementatie is dat er cyclisch en methodisch vanuit een PDCA-cyclus wordt omgegaan met informatiebeveiliging.

De onderwerpen die in de BIO worden geadresseerd zijn:

- informatiebeveiligingsbeleid en het organiseren van informatiebeveiliging
- veilig personeel, toegangsbeveiliging, fysieke beveiliging en beveiliging van de omgeving
- beheer van bedrijfsmiddelen en beveiliging bedrijfsvoering
- communicatiebeveiliging en cryptografie
- acquisitie, ontwikkeling en onderhoud van informatiesystemen en leveranciersrelaties

- beheer van informatiebeveiligingsincidenten
- informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer
- naleving

De ontwikkeling van het beleid dat de BIO voorschrijft wordt, afhankelijk van het onderwerp, door verschillende organisatieonderdelen van UWV (zogenoemde de IB&P-beleidskolommen) opgesteld. De beleidskolommen zijn HRM voor veilig personeel en autorisatiebeheer, Data Office voor gegevenshuishouding, C-ICT ten aanzien van de meer technische aspecten met betrekking tot gegevens(huishouding) en systemen en voor het IB-beleid, Facilitair Bedrijf (Huisvesting) ten aanzien van de beveiliging van gebouwen en Bureau Gegevensbescherming voor privacybeleid. De overkoepelende regie op het tot stand komen van IB-beleid ligt vooralsnog bij Bestuurszaken, maar zal in de loop van 2021 worden overgedragen aan de CIO, als nieuwe stelselverantwoordelijke.

De verschillende organisatieonderdelen zijn gehouden het vastgestelde beleid te implementeren. Ieder bedrijfsonderdeel dient zich hierover te verantwoorden in een zogenoemde 'In control verklaring', ook wel ICV. De ICV is daarmee ten behoeve van het eigen bedrijfsonderdeel om een goed en onderbouwd beeld te geven van de status van:

- De informatiebeveiliging van de bedrijfsvoering binnen de eigen directie;
- De informatiebeveiliging van de belangrijkste in- en externe partijen die relevant zijn voor de kritieke bedrijfsvoering en informatievoorziening van de eigen bedrijfsonderdeel;
- De Informatiebeveiligingsrisico's die met betrekking tot de informatievoorziening van de directie in onvoldoende mate gemitigeerd worden;
- De noodzakelijke verbetermaatregelen in de komende periode om de informatiebeveiliging te verbeteren.

Het doel is om de bedrijfsvoering van UWV veilig te maken en te houden middels het beheersen van de risico's die gerelateerd zijn aan onderwerpen uit de BIO en die samenhangen met de UWV-assets. De BIO is dus het middel om dit doel te bereiken.

Op het moment van schrijven van de laatste actualisatie van het UWV beleidskader privacy (juli 2021) wordt nog volop gewerkt aan de implementatie van de BIO en berust de documentatie nog onder het project. Deze is nog niet op DWU gepubliceerd. Wel is in bijlage I een verwijzing naar algemene informatie over de BIO opgenomen.

7.2. Toegang tot persoonsgegevens en autorisatiebeheer

Wat zegt de AVG?

De toegang tot persoonsgegevens moet goed beveiligd zijn om te voorkomen dat onbevoegden kennis kunnen nemen van persoonsgegevens en om ervoor te zorgen dat alleen die medewerkers persoonsgegevens kunnen inzien voor wie dit ook noodzakelijk is om hun taken te kunnen uitvoeren.

Artikel 5 lid 1 (c) en (f), artikel 24 lid 1 en 2, artikel 32 lid 1 (b) AVG

Zoals in hoofdstuk 3 is toegelicht, leiden de beginselen van dataminimalisatie en proportionaliteit ertoe dat bij de verwerking van persoonsgegevens ook goed gekeken moet worden naar de kring van personen die toegang hebben tot de desbetreffende persoonsgegevens. Deze personen kunnen medewerkers van UWV maar ook derden betreffen, zoals medewerkers van de gemeente of technisch beheerders van een leverancier. Daarbij geldt logischerwijs dat naarmate de persoonsgegevens gevoeliger van aard zijn (zoals gezondheidsgegevens of persoonsgegevens van strafrechtelijke aard), striktere eisen gelden voor de toegang tot die gegevens.

Naast het vaststellen van de kring van personen die toegang tot bepaalde gegevens moet hebben, moet ook aandacht worden besteed aan de vraag op welke wijze die toegang wordt verleend. Voor bepaalde persoonsgegevens met een hoge vertrouwelijkheidsklasse kan het bijvoorbeeld aangewezen zijn om toegang van buitenaf via twee-factor authenticatie te realiseren.

Het merendeel van de verwerkingen van persoonsgegevens vindt bij UWV binnen doelsystemen/applicaties plaats. De functionele toegang tot die applicaties is georganiseerd via het proces 'autorisatiebeheer'. Dit proces heeft tot doel de juiste toegangsrechten toe te kennen aan de juiste medewerkers en te bewaken dat deze

toekenningen overeen komen met de actuele functies en arbeidsplaatsen. Niet alleen het toekennen van de autorisatie, maar ook het intrekken daarvan bij uitdiensttreding van een medewerker of overstap naar een andere functie is van belang om ervoor te zorgen dat niet meer mensen toegang hebben tot persoonsgegevens dan noodzakelijk is.

Autorisatiebeheer is dus een technische maatregel om gegevens tegen ongeoorloofde toegang te beschermen en daarmee het ongeoorloofd inzien van gegevens te voorkomen. Op dit moment is binnen UWV het autorisatiebeheer geregeld volgens de richtlijn Het Proces, Normen en Controles voor 'Sluitend Autorisatiebeheer' versie 1.0 (24 november 2014). Deze richtlijn vormt een uitwerking van de normen van de BIO. Het programma Helios werkt aan een vernieuwd autorisatiebeheerproces én een bijbehorend toekomstbestendig autorisatiebeheersysteem. Zie hiervoor DWU:

<https://digitalewerkplek.sharepoint.uwv.nl/services/management/Paginas/TekstvoorVernieuwingdoorHelios.aspx>

Niet alle verwerkingen vinden echter plaats in doelsystemen die door autorisatiebeheer zijn afgeschermd. Denk bijvoorbeeld aan papieren dossiers die worden opgeslagen in een ruimte waar binnen het pand vrije toegang tot is. Of aan persoonsgegevens die aan applicaties worden onttrokken en op een andere locatie worden bewaard waar meer medewerkers of anderen toegang toe hebben. Voorbeelden hiervan zijn het bewaren van bestanden met persoonsgegevens op de G-schijf of Sharepoint of vastgelegd op een externe drager, zoals een CD-rom of USB-stick. Het gaat hier ook om afslagen van bestanden in bepaalde analyseomgevingen. Deze gegevens worden aan het autorisatiebeheer onttrokken en daarmee blootgesteld aan het risico dat ze in strijd met de beginselen van doelbinding en proportionaliteit worden verwerkt. Bovendien zijn in deze gevallen ook andere beveiligingsmaatregelen die op applicatieniveau zijn geregeld niet langer van toepassing op deze gegevens.

Het is dan ook onwenselijk dat persoonsgegevens buiten de daarvoor bestemde applicaties – meestal op ongestructureerde wijze - worden verwerkt en opgeslagen. In het project Informatie op Orde I en II wordt volop aandacht besteed aan het verwijderen van dergelijke ongestructureerde informatie van gemeenschappelijke schijven. Hoofregel is dat persoonsgegevens uitsluitend in daarvoor bestemde doelsystemen of applicaties worden verwerkt. Kunnen de desbetreffende persoonsgegevens niet in een daarvoor bestemde applicatie worden verwerkt of is er voor de desbetreffende persoonsgegevens überhaupt geen geschikte applicatie beschikbaar, dan mogen de persoonsgegevens alleen elders worden opgeslagen, indien een GEB is uitgevoerd en met de BSO is besproken. De directie dient bovendien akkoord te gaan met de afweging van risico's en maatregelen en het eventuele restrisico te accepteren. Zie hiervoor ook paragraaf 11.1.

Door het toepassen van privacy by design kan vanaf het eerste uur rekening worden gehouden met de vereisten van proportionaliteit en dataminimalisatie. Enerzijds door het systeem zo in te richten dat alleen die personen toegang hebben tot de gegevens die zij nodig hebben voor het uitvoeren van hun taken. En door voor deze geautoriseerde gebruikers de toegang te beperken tot slechts die persoonsgegevens die zij voor een specifieke verwerking nodig hebben. Bijvoorbeeld door fijnmazig autorisatiebeheer en zaakgericht werken. Hetzelfde geldt voor de toegang van geautomatiseerde processen en systemen. Via privacy by design moet ook de toegang van deze entiteiten beperkt blijven tot datgene wat noodzakelijk is voor het uitvoeren van de specifieke taak.⁵⁶ Anderzijds is het van belang dat de applicatie de noodzakelijke functionaliteit biedt om een verwerking goed te faciliteren zodat er bij gebruikers geen behoefte ontstaat om work-arounds buiten het systeem in gebruik te nemen. Het onttrekken van gegevens aan het systeem kan bovendien in bepaalde gevallen onmogelijk worden gemaakt. Denk bijvoorbeeld aan het uitschakelen van de export-functie in een applicatie.

UWV beleidskader

- **UWV zorgt er door middel van autorisatiebeheer voor dat persoonsgegevens niet breder aan medewerkers beschikbaar worden gesteld dan noodzakelijk is voor het doel van de verwerking. Op dit moment is de richtlijn Het Proces, Normen en Controles voor 'Sluitend Autorisatiebeheer' versie 1.0 (24 november 2014) daarin leidend.**
- **Het bewaren van persoonsgegevens buiten doelsystemen stelt technische beveiligingsmaatregelen zoals autorisatiebeheer buiten werking en vormt hiermee een groot risico voor (onder andere) het garanderen van proportionaliteit en dataminimalisatie in de verwerking.**

⁵⁶ CISO Office werkt aan een beleidsstuk op het gebied van Identity and Access Management (IAM) dat hier nader op in gaat.

Om die reden moet het bewaren van persoonsgegevens buiten doelsystemen zoveel mogelijk worden voorkomen. Is het bewaren van persoonsgegevens buiten een doelsysteem noodzakelijk omdat de bestaande doelsystemen of applicaties verwerking ervan niet mogelijk maken, dan moet een GEB worden uitgevoerd en met de BSO worden besproken. De directie dient akkoord te zijn met de voorgestelde maatregelen op de benoemde risico's en het eventuele restrisico te accepteren. Dit geldt ook voor het bewaren van persoonsgegevens in fysieke documenten – ook hier moet het toegangsbeheer aan de beginselen van de AVG voldoen.

- Door middel van privacy by design moet vanaf het eerste uur rekening worden gehouden met de vereisten van proportionaliteit en dataminimalisatie.

7.3. Classificeren van gegevens (BIV-classificatie)

De AVG verlangt van UWV dat persoonsgegevens adequaat worden beveiligd.⁵⁷ Het BIV-classificatiedocument 2.0 (zie de bijlage voor de locatie op DWU) is een belangrijk instrument in de afweging van wat voor UWV een adequaat niveau van beveiliging is.

Het classificeren van gegevens houdt in dat deze aan de hand van een analyse worden ingedeeld in verschillende niveaus van drie informatiebeveiligingsprincipes: beschikbaarheid, integriteit en vertrouwelijkheid. Op elk van deze beveiligingsprincipes bepaalt het belang van de gegevens welk classificatieniveau van toepassing is. Het aldus vastgestelde classificatieniveau maakt mede inzichtelijk welk beschermingsniveau geboden is, zodat gerichte maatregelen kunnen worden getroffen om de gegevens adequaat te beschermen tegen onrechtmatige inzage, wijziging, verlies of onbeschikbaarheid.

Ook persoonsgegevens worden geclassificeerd. De vertrouwelijkheidsklasse van persoonsgegevens is minimaal klasse 2. Bijzondere persoonsgegevens zijn extra gevoelig en moeten daarom ook extra vertrouwelijk worden behandeld. Deze gegevens krijgen daarom minimaal vertrouwelijkheidsklasse 2+ toegekend. Binnen deze groep extra gevoelige gegevens wordt ten slotte ook nog een groep gegevens onderkend die strikt vertrouwelijk moeten worden behandeld. Dit zijn bijvoorbeeld gezondheidsgegevens die normaliter in het dossier van een arts zijn opgenomen, zoals een diagnose, gegevens met betrekking tot een onderzoek dat naar een persoon is ingesteld - bijvoorbeeld in verband met mogelijke fraude en VIP-gegevens. Voor deze gegevens geldt vertrouwelijkheidsklasse 3. Deze gegevens dienen in de systemen van UWV goed te zijn afgescheiden van andere gegevens.

In het BIV-classificatiedocument 2.0 wordt uitgebreid ingegaan op het belang van gegevensclassificatie, welke klassen worden onderscheiden en hoe moet worden geclassificeerd. Is het classificatieniveau vastgesteld, dan kan mede op basis daarvan worden bepaald welke beveiligingsmaatregelen moeten worden getroffen om de gegevens adequaat te beveiligen.

Ten aanzien van het bepalen van een adequaat niveau van toegangsbeveiliging, kan daarnaast gewezen worden op de Handleiding betrouwbaarheidsniveaus voor digitale dienstverlening die speciaal voor overheidsdiensten is opgesteld.⁵⁸

Hoewel de AVG financiële gegevens niet afzonderlijk noemt als gegevens die extra gevoelig zijn, moet ook met dergelijke gegevens bijzonder voorzichtig worden omgesprongen.⁵⁹ UWV verwerkt van klanten, personen in de polisadministratie en medewerkers gevoelige financiële gegevens. De hoogte van het inkomen of vermogen van een persoon of het feit dat iemand een uitkering of schulden heeft, zijn gegevens die privacygevoelig zijn en dus extra goed beschermd moeten worden. Ook een bankrekeningnummer is gevoelig omdat het – in combinatie met enkele andere gegevens van de betrokkene – gemakkelijk misbruikt kan worden door derden.

⁵⁷ Artikel 5 lid 1 sub (f) en artikel 32 AVG

⁵⁸ Opgesteld door Forum Standaardisatie.

⁵⁹ Zie Handleiding AVG van de Rijksoverheid, p. 26. <https://www.rijksoverheid.nl/documenten/rapporten/2018/01/22/handleiding-algemene-verordening-gegevensbescherming>

7.4. Veilig communiceren van persoonsgegevens

In paragraaf 2.2 is aangegeven dat het verstrekken, versturen, doorzenden, verspreiden en delen van persoonsgegevens aan de betrokkene of aan de bevoegde derde een verwerking is die aan de beginselen van de AVG moet voldoen. Dit betekent dat voorafgaand aan de vraag welk communicatiemiddel geschikt is om de gegevens te delen, altijd eerst moet worden vastgesteld dat de gegevens überhaupt met de ontvangende partij mogen worden gedeeld. Zie hiervoor ook paragraaf 5.6.

Wanneer dit is vastgesteld, moet een veilige manier worden gevonden om de persoonsgegevens te verstrekken. Hierbij moet een onderscheid worden gemaakt tussen de interne communicatie waarbij persoonsgegevens aan collega's van UWV worden verstrekt en externe communicatie waarbij persoonsgegevens aan derden worden verstrekt.

Deze paragraaf gaat over communicatie waarbij persoonsgegevens worden gedeeld/verstrekkt. De beleidsuitspraken die hieronder worden gedaan, gelden dus niet voor de communicatie waarin geen sprake is van het verstrekken van persoonsgegevens of van andere vertrouwelijke bedrijfsinformatie.

7.4.1. Interne communicatie met collega's van UWV

De beste manier om persoonsgegevens met collega's binnen UWV te delen is door het gezamenlijk gebruik van doelsystemen. Door middel van autorisatiebeheer is geregeld dat alleen die collega's toegang hebben tot de persoonsgegevens die deze nodig hebben voor de uitvoering van hun taken.

Maar lang niet in alle gevallen wordt er gezamenlijk gewerkt in doelsystemen. In de praktijk wordt bijvoorbeeld aan stafmedewerkers per e-mail casuïstiek voorgelegd waarbij persoonsgegevens van de betreffende casus worden gedeeld om de vraag toe te lichten. Of bij het verdelen of overdragen van werk in een team worden BSN's en namen van klanten per e-mail gedeeld. Ook komt het voor dat met betrekking tot een dossier advies wordt ingewonnen bij een andere divisie. Bijvoorbeeld ten aanzien van het uitkeringsrecht of de beoordeling door de verzekeringsarts of arbeidsdeskundige.

Het intern mailen tussen UWV-collega's met UWV-Outlookaccounts is technisch gezien een veilige manier van communiceren en kan dus worden gebruikt om persoonsgegevens met een collega te delen die die gegevens nodig heeft voor de uitvoering van zijn of haar taken. Collega's kunnen dus onderling op een veilige manier communiceren via de interne e-mail.

Toch kleeft er ook aan intern mailen een aantal risico's die zelfs kunnen leiden tot een datalek. Daarom moeten een aantal waarborgen in acht worden genomen.

Ten eerste bestaat het risico dat door typefouten of de autoaanvullingsfunctie van Outlook per ongeluk een verkeerd emailadres van een ander wordt geselecteerd en daarmee een potentieel datalek wordt gecreëerd. Wanneer je ook via mail met derden communiceert kan zo'n voorgeselecteerd adres ook van een externe partij zijn. Het verdient daarom de voorkeur om autoaanvulling uit te schakelen. Bij het intern versturen van veel of gevoelige persoonsgegevens is het raadzaam om een extra check te doen.

Daarnaast leent e-mail zich goed om stukken met een enkele druk op de knop door te sturen. Hierdoor bestaat het risico dat het verzonden bericht niet bij de ontvanger blijft, maar vanuit daar met meer personen wordt gedeeld. Met dit risico moet rekening worden gehouden bij het gebruik van e-mail. Als een mail wordt doorgestuurd, moet ook kritisch worden gekeken of het nodig is om alle gegevens door te sturen. Onnodige informatie moet uit de mail worden verwijderd.

Ook de Outlookautorisaties – die medewerkers zelf kunnen aanwijzen – brengen risico's met zich mee. Door collega's te autoriseren hebben zij mogelijk toegang tot gegevens waartoe zij geen toegang zouden mogen hebben.

Deze kanttekeningen bij het gebruik van e-mail pleiten voor terughoudendheid bij het delen van persoonsgegevens via email, zeker waar dat gevoelige persoonsgegevens of grote bestanden betreft.

Een extra beveiligingsmaatregel kan zijn om een eventuele bijlage te versleutelen en met een wachtwoord te beveiligen dat op een andere manier aan de ontvanger wordt verstrekt.

7.4.2. Externe communicatie met derden

UWV heeft veel contacten met externe partijen, zoals met klanten, werkgevers, leveranciers, re-integratiebureaus, gemeenten, artsen, advocaten etc. Zeker wanneer met dergelijke partijen (gevoelige) persoonsgegevens worden gedeeld, is het van belang te verzekeren dat de communicatie op een veilige manier plaatsvindt.

Schriftelijk

Bij het e-mailen met derden spelen dezelfde risico's als hierboven bij intern mailen zijn benoemd. Daar komt echter bij dat op dit moment de gewone e-mail aan derden onvoldoende beveiligd is tegen aftappen en hacken, waardoor de geheimhoudingsplicht van UWV zou kunnen worden geschonden.

Voor schriftelijke communicatie waarbij persoonsgegevens worden verstrekt/gedeeld geldt het volgende beleid:

- Er is een aantal veilige digitale communicatiekanalen beschikbaar, zoals de werkmap, mijn berichtenbox en mijn gegevensdiensten. Waar mogelijk worden deze veilige communicatiekanalen gebruikt voor de communicatie met klanten, werkgevers en afnemers van gegevensleveringen. Afhankelijk van de vertrouwelijkheidsklasse kunnen deze kanalen ook worden gebruikt voor communicatie waarbij persoonsgegevens worden gedeeld.
- Als er geen van deze veilige digitale communicatiekanalen beschikbaar zijn, wordt voor het verstrekken van persoonsgegevens gebruik gemaakt van de post.
- Is het praktisch niet mogelijk om van de post gebruik te maken, bijvoorbeeld omdat bepaalde (wettelijke) termijnen dan niet gehaald worden, dan moet het betreffende organisatieonderdeel voor dit werkproces middels het GEB-proces een afweging maken om in het concrete geval wel van de e-mail gebruik te maken. Daarbij moeten dan zoveel mogelijk maatregelen worden getroffen om het risico van het gebruik van de mail te verkleinen. Bijvoorbeeld door het gebruik van Zivver, dat binnen UWV breed is uitgerold. Zivver versleutelt berichten zodat ze als ze onderweg worden onderschept niet leesbaar zijn. Daarnaast werkt Zivver met 2-factorauthenticatie en kunnen berichten ingetrokken. Meer informatie over Zivver vind je op de DWU-pagina van programma Iris:

<https://digitalewerkplek.sharepoint.uwv.nl/uwv/programmas-en-projecten/Paginas/ProgrammaIris.aspx>

Mondeling

Wanneer informatie over een klant of medewerker mondeling wordt gedeeld, bijvoorbeeld over de telefoon, is het van groot belang dat is verzekerd dat de juiste persoon die informatie ontvangt. Ook dit is van belang om te voorkomen dat UWV zijn geheimhoudingsplicht schendt. Daarom moet de medewerker van UWV zich ervan verzekeren dat hij of zij de juiste persoon tegenover zich of aan de lijn heeft, voordat (vertrouwelijke) persoonsgegevens worden gedeeld. K&S beschikt hiertoe over een protocol voor outbound telefonie.

UWV beleidskader

- **UWV volgt de Baseline Informatiebeveiliging Overheid (BIO) voor de implementatie van technische en organisatorische beveiligingsmaatregelen.**
- **Bij het bepalen van adequate beveiligingsmaatregelen maken de organisatieonderdelen gebruik van de BIV-classificatie. Aan de hand hiervan wordt bepaald in welke vertrouwelijkheidsklasse de persoonsgegevens die worden verwerkt vallen. Hoe hoger de vertrouwelijkheidsklasse, hoe zwaarder de beveiligingsmaatregelen.**
- **E-mail binnen UWV is een veilig communicatiekanaal. Wanneer echter per mail persoonsgegevens worden verstuurd, dan moet dit tot een minimum worden beperkt.**
- **Om verkeerde adressering van e-mails te voorkomen, verdient het aanbeveling om auto-aanvulling in Outlook uit te schakelen.**
- **E-mail met derden buiten UWV is in principe niet veilig. Daarom wordt het versturen van persoonsgegevens aan derden via open e-mail tot een absoluut minimum beperkt. Indien het toch nodig is om met externen te mailen en daarbij persoonsgegevens te delen, maak dan gebruik van Zivver.**

-
- Daar waar veiliger kanalen voor communicatie met derden bestaan, zoals de werkmap, mijn berichtenbox e.d. moet altijd voor deze kanalen worden gekozen.
 - Grote bestanden met veel persoonsgegevens worden nooit onversleuteld per e-mail verzonden.

8. Transparantie en verantwoording

Een belangrijk uitgangspunt bij de zorgvuldige omgang met persoonsgegevens is dat organisaties die persoonsgegevens verwerken hierover transparant zijn richting de betrokkene, dat wil zeggen de persoon van wie persoonsgegevens worden verwerkt. Daarom vereist de AVG dat de betrokkene actief wordt geïnformeerd over de verwerking van zijn persoonsgegevens en over zijn rechten. Dit kan bijvoorbeeld door het verwijzen naar of verstrekken van een privacyverklaring (paragraaf 8.1).

Daarnaast vereist de AVG dat organisaties zelf kunnen aantonen dat ze aan de eisen van de AVG voldoen ('compliant zijn'). Van organisaties die in belangrijke mate persoonsgegevens verwerken – zoals UWV – wordt vereist dat zij een passend privacybeleid hebben.⁶⁰ Ook vereist de AVG dat organisaties inzicht hebben in de verwerkingen van persoonsgegevens die zij hebben. Dit inzicht moet worden aangetoond aan de hand van een register van verwerkingen dat moet worden opgesteld en moet worden bijgehouden (paragraaf 8.2). Verder kent de AVG een aantal andere bepalingen die organisaties helpen om naleving van de AVG aan te tonen. In dit verband kunnen worden genoemd: het aanstellen van een functionaris voor de gegevensbescherming (hoofdstuk 10), het uitvoeren van GEB's (paragraaf 11.1) en het melden van beveiligingsincidenten en datalekken (paragraaf 11.2).

8.1. Informatie over de verwerking aan betrokkene (privacyverklaring)

Wat zegt de AVG?

Degene die persoonsgegevens van een betrokkene verzamelt, moet de betrokkene hierover informeren. De informatie moet onder andere inzicht geven in het doel van de verwerking en de wijze waarop zijn persoonsgegevens worden verwerkt.

Artikel 12, 13 en 14 AVG

De AVG schrijft zeer gedetailleerd voor welke informatie aan een betrokkene moet worden verstrekt, wanneer een organisatie persoonsgegevens van hem of haar gaat verwerken. Het gaat zowel om de situatie dat de persoonsgegevens bij de betrokkene zelf worden verzameld⁶¹ (bijv. wanneer een klant een uitkering aanvraagt) als om de situatie dat persoonsgegevens over de betrokkene bij een derde worden verzameld⁶² (bijv. gegevens die UWV over een klant van de werkgever ontvangt), tenzij die gegevens op basis van een wettelijke verplichting van die derde zijn ontvangen.

De informatie die UWV aan de betrokkene moet verstrekken voorafgaand aan het verzamelen van de persoonsgegevens is de volgende:

- het doel of de doelen van de verwerking (zie paragraaf 3.3);
- de rechtsgrond voor de verwerking (zie hoofdstuk 4);
- of de betrokkene verplicht is (op basis van de wet of een contract) persoonsgegevens te verstrekken en wat de gevolgen zijn als hij dit weigert;
- de bewaartermijn voor de gegevens of de criteria op grond waarvan de bewaartermijn wordt bepaald (dit zijn voor UWV de bewaartermijnen uit de selectielijst van UWV, zie hoofdstuk 6)
- de rechten die betrokkene heeft (bijv. recht op inzage en correctie, klacht indienen bij de AP, zie hoofdstuk 9);
- de contactgegevens van UWV en van de Functionaris Gegevensbescherming.

Naast bovengenoemde informatie, moet UWV in bepaalde gevallen de volgende aanvullende informatie aan de betrokkene verstrekken:

⁶⁰ Artikel 24 lid 1 en 2 AVG.

⁶¹ Artikel 13 AVG.

⁶² Artikel 14 AVG.

- indien gebruik wordt gemaakt van geautomatiseerde besluitvorming met rechtsgevolgen voor de betrokkene, een omschrijving daarvan alsmede de onderliggende logica (in begrijpelijke taal) (zie paragraaf 5.8.3);
- indien de gegevens worden verstrekkt aan een derde, een omschrijving van die derden;
- indien UWV voornemens is de gegevens voor een ander doel te verwerken, informatie over dat andere doel en de rechtsgrond (zie paragraaf 3.3);
- indien het voornemen bestaat de persoonsgegevens te verstrekken aan een land buiten de EER⁶³ of een internationale organisatie, de waarborgen die zijn getroffen om de privacy van de betrokkene in dat land te waarborgen (paragraaf 5.6);
- indien de verwerking plaatsvindt op de grondslag van gerechtvaardigd belang, een beschrijving van dat gerechtvaardigde belang (zie paragraaf 4.4);
- indien de verwerking plaatsvindt op grond van toestemming, dat de betrokkene het recht heeft te allen tijde zijn toestemming in te trekken (zie hiervoor paragraaf 4.6);
- Indien de persoonsgegevens zijn verkregen van een derde (i.p.v. van de betrokkene zelf), de beschrijving van die derde.

Deze informatie hoeft slechts éénmaal te worden verstrekt aan de betrokkene.⁶⁴ Dit moet gebeuren op het moment dat de persoonsgegevens bij de betrokkene worden verzameld. De informatie moet schriftelijk - op papier of digitaal - worden verstrekt of met gebruikmaking van andere middelen. Verder moet de informatie in een begrijpelijk, toegankelijke vorm en in duidelijke en eenvoudige taal worden gegeven.

Voor zijn klanten heeft UWV een privacyverklaring gepubliceerd op de website. Onderdeel van die privacyverklaring is een overzicht van persoonsgegevens die UWV van zijn klanten verwerkt (klantvriendelijk register van verwerkingen) (zie bijlage). Op het moment dat persoonsgegevens bij de betrokkene worden uitgevraagd, moet de betrokkene hierop worden gewezen. Voor niet-digitaalvraagende klanten is een papieren variant van de privacyverklaring beschikbaar. Deze moet aan de betrokkene worden verstrekt op het moment dat hij hem of haar voor het eerst gegevens worden uitgevraagd. Voor klanten die de Nederlandse taal niet machtig zijn wordt in 2021 een Engelse versie van de privacyverklaring gepubliceerd.

De verplichting om een privacyverklaring te overleggen geldt niet alleen voor klanten van UWV, maar ook voor andere betrokkenen waar UWV persoonsgegevens van verwerkt.

Op uwv.nl is naast de privacyverklaring voor klanten ook een privacyverklaring voor werkgevers en voor evenementen gepubliceerd. Er wordt nog gewerkt aan een privacyverklaring voor zakelijke relaties, een voor begeleiders van klanten en voor sollicitanten.

Op DWU is sinds juni 2021 de privacyverklaring voor medewerkers van UWV te vinden.

Zie bijlage I voor de precieze locaties van deze verklaringen.

De plicht om de betrokkene te informeren over de verwerking van zijn of haar persoonsgegevens geldt ook wanneer die gegevens niet van de betrokkene zelf zijn ontvangen, maar van een derde zoals bijvoorbeeld de arts van betrokkene. Op deze verplichting bestaan enkele uitzonderingen.⁶⁵ Zo hoeft UWV de betrokkene niet te informeren over de verwerking van *van een derde ontvangen* persoonsgegevens:

- wanneer de persoonsgegevens aan UWV zijn verstrekt op basis van een wettelijke verplichting die op die derde rust (dit zal bij UWV vaak het geval zijn);
- wanneer de verstrekking van de persoonsgegevens aan UWV vertrouwelijk moet blijven in verband met het beroepsgeheim dat rust op degene die de gegevens aan UWV verstrekt (dit kan het geval zijn wanneer UWV informatie over een klant van de politie ontvangt);
- wanneer het persoonlijk informeren van de betrokkene praktisch onmogelijk is of dit van UWV een disproportionele inspanning zou vergen.

In dat laatste geval moet de informatie zoals hierboven beschreven wél openbaar worden gemaakt, bijvoorbeeld via een website.

⁶³ De EER bestaat uit de lidstaten van de EU, Noorwegen, IJsland en Liechtenstein.

⁶⁴ Artikel 13 lid 4 AVG.

⁶⁵ Artikel 14 lid 5 AVG.

8.2. Register van verwerkingen

Wat zegt de AVG?

Iedere organisatie die persoonsgegevens verwerkt moet een register van verwerkingen aanleggen en bijhouden. Dit register bevat belangrijke informatie over bijvoorbeeld het doel van de verwerking, de persoonsgegevens die worden verwerkt, aan wie persoonsgegevens worden verstrekt, bewaartermijnen en getroffen beveiligingsmaatregelen.

Artikel 30 AVG

Het register van verwerkingen is bedoeld voor organisaties om richting de toezichthouder (de Autoriteit Persoonsgegevens) te kunnen aantonen over welke verwerkingen van persoonsgegevens die organisatie beschikt.

De gegevens die in het register van verwerkingen moeten worden opgenomen ten aanzien van verwerkingen waarvoor UWV verwerkingsverantwoordelijke is, zijn de volgende:

- naam en contactgegevens van de verwerkingsverantwoordelijke (voor UWV is dit de voorzitter van de Raad van Bestuur) en van de Functionaris Gegevensbescherming;
- verwerkingsdoeleinden ('waarom verwerkt UWV de persoonsgegevens?');
- beschrijving van de categorieën van personen over wie persoonsgegevens worden verwerkt;
- beschrijving van de categorieën van persoonsgegevens;
- beschrijving van de categorieën van organisaties aan wie persoonsgegevens worden verstrekt;
- zo mogelijk, de bewaartermijnen die gelden voor de persoonsgegevens;
- zo mogelijk, een algemene beschrijving van technische en organisatorische beveiligingsmaatregelen;
- indien van toepassing, of persoonsgegevens worden verstrekt aan een organisatie in een land buiten de EER en eventueel de passende waarborgen die in dit verband moeten worden genomen.

Ook de verwerkingen waarvan UWV verwerker (en dus niet verwerkingsverantwoordelijke) is, moeten in het register van verwerkingen worden opgenomen (zie artikel 30 lid 2 AVG).

Het register van verwerkingen van UWV moet alle verwerkingen van persoonsgegevens van UWV bevatten. Dus naast de verwerkingen van persoonsgegevens van klanten, moeten ook alle andere verwerkingen van persoonsgegevens, zoals bijvoorbeeld van medewerkers, daarin worden opgenomen.

UWV heeft een register van verwerkingen opgesteld dat op DWU is te raadplegen. Zie bijlage I voor de precieze locatie van het register. Er is een procedure voor het actueel houden van het register (zie paragraaf 11.4).

UWV beleidskader

- **UWV stelt privacyverklaringen op voor alle relevante categorieën van personen (klanten, medewerkers, sollicitanten en andere relaties van UWV) van wie UWV persoonsgegevens verwerkt. Voor niet-digivaardigen is een papieren versie beschikbaar.**
- **Op het moment dat persoonsgegevens bij de betrokkene worden uitgevraagd, wordt aan hem of haar de desbetreffende privacyverklaring verstrekt of hij of zij wordt op dat moment via een link verwezen naar de digitale privacyverklaring.**
- **UWV heeft een register van verwerkingen. In dat register moeten alle verwerkingen van UWV zijn opgenomen. Dit geldt zowel voor de verwerkingen waarvoor UWV verwerkingsverantwoordelijke is als voor verwerkingen waarvoor UWV verwerker is.**
- **Om het register actueel te houden, geeft ieder organisatieonderdeel wijzigingen of aanvullingen van het register door aan team IB&P BZ via het daarvoor beschikbare formulier.**
- **Op verzoek verstrekt de FG het register aan de Autoriteit Persoonsgegevens.**

9. Rechten van betrokkenen

Burgers vinden het steeds belangrijker om controle te kunnen uitoefenen op de verwerking van hun persoonsgegevens. Daarvoor is in de eerste plaats nodig dat zij goed geïnformeerd worden over die verwerking. Daarom verplicht de AVG om personen actief te informeren over de verwerking van hun gegevens (zie paragraaf 8.1, privacyverklaring).

Daarnaast zijn de rechten van betrokkenen door de AVG verder uitgebreid om hun controlemogelijkheden te vergroten. Nog even voor de duidelijkheid: een 'betrokkene' is de persoon op wie de persoonsgegevens betrekking hebben. Voorbeelden van betrokkenen bij UWV zijn de klanten van UWV, personen die in de polisadministratie staan geregistreerd, medewerkers van UWV of contactpersonen van leveranciers. De betrokkene heeft de volgende rechten.

- De betrokkene kan vragen of UWV persoonsgegevens over hem of haar verwerkt en zo ja, om die gegevens in te zien (paragraaf 9.1).
- De betrokkene kan vragen om zijn gegevens te corrigeren als ze onjuist of onvolledig zijn (paragraaf 9.2).
- De betrokkene kan vragen om zijn persoonsgegevens te vernietigen. Alleen in bepaalde gevallen moet UWV aan zo'n verzoek voldoen (paragraaf 9.3).
- De betrokkene kan in bepaalde gevallen vragen om de verwerking van zijn gegevens tijdelijk stil te leggen. Dit heet het recht op beperking van de verwerking (paragraaf 9.4).
- De betrokkene kan bezwaar maken tegen de verwerking (paragraaf 9.5).

Naast deze rechten kent de AVG ook nog het recht op overdraagbaarheid van persoonsgegevens ('data-portabiliteit'), maar dit recht is niet van toepassing op persoonsgegevens die UWV verwerkt ter uitvoering van zijn publiekrechtelijke taak. Het recht van data-portabiliteit geldt alleen voor gegevens die op de grondslag 'toestemming' of 'uitvoering overeenkomst' worden verwerkt. Waar die grondslag wordt gebruikt (bijv. de verwerking van personeelsgegevens door UWV als werkgever) is data-portabiliteit dus wel van toepassing als ook aan de andere voorwaarden van artikel 20 lid 1 AVG is voldaan.

Reactietermijn

Binnen 5 dagen na ontvangst van het verzoek, stuurt UWV een ontvangstbevestiging aan de verzoeker. De verzoeken moeten in principe binnen een maand na ontvangst zijn beantwoord. Als het een complex verzoek is, kan die termijn met twee maanden worden verlengd.⁶⁶

Overleg met betrokkene

Indien een verzoek onduidelijk of complex is of indien een verzoek wordt gedaan tot correctie of verwijdering van gegevens waaraan UWV niet kan voldoen, wordt aangeraden om in overleg te treden met de verzoeker. Zo kan beter de bedoeling achter het verzoek worden achterhaald, waardoor het verzoek bijvoorbeeld specifieker kan worden gemaakt, op andere wijze aan bezwaren van de betrokkene kan worden voldaan of kan worden uitgelegd waarom niet aan het verzoek kan worden voldaan.

Kosten

Voor de behandeling van verzoeken en de beantwoording daarvan worden aan de betrokkene géén kosten in rekening gebracht.⁶⁷

Informatie aan derden

Als UWV voldoet aan een verzoek tot correctie, verwijdering of stillegging van de verwerking en het gaat om persoonsgegevens die aan een andere organisatie of instelling zijn verstrekt, dan moet UWV in principe die andere organisatie daarvan op de hoogte stellen.⁶⁸ Belangrijke uitzondering op deze informatieplicht is wanneer het voldoen hieraan onmogelijk is of een onevenredige inspanning zou vergen.

⁶⁶ Artikel 12 lid 3 AVG.

⁶⁷ Artikel 12 lid 5 AVG.

⁶⁸ Artikel 19 AVG.

9.1. Verzoek om inzage in persoonsgegevens

Wat zegt de AVG?

De betrokkene heeft het recht om antwoord te krijgen op de vraag of over hem of haar persoonsgegevens worden verwerkt en, bij een bevestigend antwoord, om inzage te krijgen in die persoonsgegevens. Wanneer de betrokkene daarom vraagt, ontvangt hij of zij een kopie van de gegevens. Daarbij moet wel rekening worden gehouden met de privacy van anderen die mogelijk kan worden geschonden als een kopie wordt verstrekt.

Artikel 15 en 16 AVG, Regeling inzage- en correctierecht UWV 2018 (Stcrt. 2018, 28604)

Als een betrokkene daarom vraagt moet UWV antwoord geven op de vraag of persoonsgegevens van hem of haar worden verwerkt. Vervolgens moet UWV de betrokkene de mogelijkheid bieden om zijn of haar gegevens in te zien en - indien de betrokkene daarom verzoekt - een kopie daarvan te geven.

Naast het feit dat de betrokkene de mogelijkheid moet worden gegeven om zijn of haar persoonsgegevens in te zien, moet UWV ook in staat zijn desgevraagd de volgende informatie daarbij te verstrekken:

- de doeleinden voor de verwerking,
- de categorieën van persoonsgegevens die worden verwerkt,
- de bewaartermijn die voor de desbetreffende persoonsgegevens geldt,
- de rechten die de betrokkene heeft (correctie, verwijdering, stilleggen, bezwaar maken, klacht indienen bij AP).

In bepaalde gevallen moet ook nog aanvullende informatie worden verstrekt. Dit is het geval:

- indien de persoonsgegevens zijn of worden verstrekt aan andere organisaties of instellingen, de namen van deze organisaties of de categorieën van organisaties,
- indien de persoonsgegevens afkomstig van een andere organisatie of instelling zijn, van welke organisatie of instelling die persoonsgegevens afkomstig zijn (de bron),
- indien de persoonsgegevens worden verwerkt in een proces waarin gebruik wordt gemaakt van volledig geautomatiseerde besluitvorming, de onderliggende logica van dat proces en de gevolgen voor de betrokkene,
- indien de persoonsgegevens worden verstrekt aan een organisatie of instelling in een derde land buiten de EU, op grond van welke verdragsbepaling deze gegevens zijn vertrekt.

Voor de volledigheid wordt nog opgemerkt dat de betrokkene met een AVG-inzageverzoek geen informatie kan opvragen over welke medewerker van UWV een bepaald dossier heeft ingezien of bewerkt. Deze informatie valt niet onder de persoonsgegevens van de betrokkene die hij mag inzien. Dit is anders indien een betrokkene op basis van de WGBO een verzoek om inzage in zijn medisch dossier doet. Het inzagerecht onder de WGBO is ruimer geformuleerd. In die gevallen is UWV wel verplicht om te delen wie het medisch dossier heeft geraadpleegd.⁶⁹

UWV heeft het proces van het inzage- en correctierecht vastgesteld in de Regeling inzage- en correctierecht UWV 2018. Deze Regeling is gepubliceerd in de Staatscourant.⁷⁰ Sinds 2021 is het voor klanten mogelijk om hun inzageverzoek via uwv.nl te doen. Hiervoor is een webformulier achter DigiD beschikbaar.

Op DWU is een pagina met overzichtelijke informatie over het inzage- en correctierecht beschikbaar en zijn er voor de medewerkers van UWV procedures en instructies opgesteld over de wijze waarop een verzoek om inzage of correctie moet worden afgehandeld. Zie DWU Handboek 'proces informatie verstrekken' onderdeel 'behandelen verzoek om inzage'. Ten slotte zal in Q3 2021 een Handreiking inzagerecht verschijnen om organisatieonderdelen te ondersteunen bij de afhandeling van inzageverzoeken. Zie voor de locatie van deze documenten bijlage I.

Twee punten uit de hierboven genoemde instructies worden hier vanwege hun belang nog apart vermeld:

⁶⁹ Artikel 7:456 BW

⁷⁰ Staatscourant 2018, nr. 28604.

- Een verzoek om inzage in gegevens uit een medisch dossier wordt doorgezonden naar het betrokken onderdeel van Sociaal Medische Zaken (SMZ) en beoordeeld door de verzekeringsarts krachtens de aanwijzingen van de Richtlijn Beheer medische gegevens vallend onder het medisch beroepsgeheim van de verzekeringsarts.
- Een verzoek om inzage in gegevens uit een handhavingss dossier wordt doorgezonden naar de directie Handhaving (DHH), die deze beoordeelt volgens de instructie DHH Inzage-en correctierecht. Er wordt door de afdeling waar het verzoek is binnen gekomen niet aan betrokkene bevestigd dat er een handhavingss dossier bestaat – ook dit is aan DHH.

9.2. Verzoek om correctie van persoonsgegevens

Wat zegt de AVG?

Een betrokkene heeft het recht om te verzoeken om onjuiste of onvolledige gegevens over hem of haar te laten corrigeren of aanvullen.

Artikel 16 AVG, Regeling inzage- en correctierecht UWV 2018 (Stcrt 2018, 28604)

Indien de betrokkene van oordeel is dat de persoonsgegevens onjuist zijn, heeft hij het recht om deze te laten corrigeren. Bij onvolledigheid kan hij verzoeken de persoonsgegevens aan te vullen, bijvoorbeeld door middel van het opnemen van een verklaring.

UWV kent verschillende procedures voor klanten om persoonsgegevens te wijzigen. Via mijnUWV bijvoorbeeld kunnen wijzigings- en correctieverzoeken worden ingediend. Dergelijke verzoeken maken onderdeel uit van het primaire proces van UWV. Ze moeten daarom onderscheiden worden van verzoeken tot correctie op basis van de AVG. Bij een correctieverzoek op basis van de AVG gaat het om persoonsgegevens die niet binnen het reguliere proces kunnen worden gewijzigd.

UWV heeft het proces van het inzage- en correctierecht vastgesteld in de in paragraaf 9.1 genoemde *Regeling inzage- en correctierecht UWV 2018*. In de handboeken van UWV zijn procedures en instructies voor de medewerkers opgenomen zodat zij weten hoe te handelen in geval van een verzoek om correctie of aanvulling van gegevens. Zie DWU Handboek 'proces informatie verstrekken' onderdeel 'behandelen verzoek om correctie'.

Ook een verzoek om correctie van gegevens uit een medisch dossier wordt doorgezonden naar het betrokken onderdeel van Sociaal Medische Zaken (SMZ) en beoordeeld door de verzekeringsarts krachtens de aanwijzingen van de Richtlijn Beheer medische gegevens vallend onder het medisch beroepsgeheim van de verzekeringsarts.

Een verzoek om correctie van gegevens uit een uit een handhavingss dossier wordt doorgezonden naar de directie Handhaving (DHH) en beoordeeld volgens de instructie DHH Inzage-en correctierecht.

Lang niet alle persoonsgegevens die UWV verwerkt kan UWV voor de klant corrigeren. Zo kan UWV bijvoorbeeld gegevens die zijn opgenomen in de polisadministratie niet zelf aanpassen. De polisadministratie wordt namelijk gevuld met gegevens uit de loonaangifte afkomstig van de inhoudingsplichtige/werkgever. Deze is verantwoordelijk voor de juiste invulling. UWV dient correcties met betrekking tot loongegevens of het ten onrechte ontbreken van een dienstverband te melden aan de Belastingdienst. De Belastingdienst onderneemt dan actie richting inhoudingsplichtige/werkgever. De inhoudingsplichtige/werkgever wordt dan verzocht een correctiebericht in te sturen. Een ander voorbeeld is correctie van adresgegevens die UWV ontvangt uit de Basisregistratie personen (BRP). Hiervoor zal de klant moeten worden doorverwezen naar de gemeente.

9.3. Verzoek om verwijdering van persoonsgegevens

Wat zegt de AVG?

Een betrokkene heeft het recht om te verzoeken gegevens over hem of haar uit de systemen te laten verwijderen. Alleen in bepaalde gevallen is een organisatie verplicht aan dit verzoek te voldoen, bijvoorbeeld indien de verwerking niet rechtmatig is omdat de bewaartermijn is verstreken.

Artikel 17 AVG

Dit recht wordt ook wel het 'recht op vergetelheid' genoemd. Het gaat er kort gezegd om dat de betrokkene een verzoek kan doen om persoonsgegevens te vernietigen. Alleen in bepaalde gevallen is een organisatie verplicht om aan zo'n verzoek te voldoen, namelijk als de verwerking niet of niet langer rechtmatig is. Ook UWV kan onder omstandigheden verplicht zijn aan een verzoek tot het vernietigen van gegevens te voldoen.

Volgens de AVG moet aan een verzoek tot vernietiging worden voldaan als de gegevens niet langer nodig zijn dan voor de doeleinden waarvoor ze worden verwerkt.⁷¹ Zoals echter in hoofdstuk 6 is toegelicht, geldt voor UWV de Archiefwet en andere wetgeving die UWV verplicht gegevens gedurende een bepaalde termijn te bewaren. Dit betekent dat UWV in principe niet aan een verzoek tot vernietiging zal kunnen voldoen zolang de archiefwetgeving en de daarop gebaseerde selectielijst UWV verplicht de gegevens langer te bewaren. Deze uitzonderingsgrond wordt ook in de AVG genoemd.⁷² Dit betekent dat wanneer een verzoek om verwijdering betrekking heeft op persoonsgegevens die UWV verwerkt ter uitvoering van zijn wettelijke taak en waarvan de bewaartermijn die is opgenomen in de selectielijst UWV nog niet is verstreken, het verzoek tot vernietigen in principe wordt afgewezen. Wanneer echter de bewaartermijn wel is verstreken en de gegevens staan onverhoopt nog in de systemen van UWV, dan zal wél aan het verzoek gehoor moeten worden gegeven en moeten de gegevens alsnog worden vernietigd.⁷³

Ook wanneer de bewaartermijn nog niet is verstreken, kunnen zich gevallen voordoen waarin UWV toch aan een verzoek tot vernietiging moet voldoen. Dit is aan de orde als UWV de persoonsgegevens onrechtmatig verwerkt omdat er geen grondslag voor de verwerking bestaat (zie hoofdstuk 4) of omdat niet aan een van de andere privacybeginselen van de AVG wordt voldaan (zie hoofdstuk 3). Een voorbeeld hiervan zou kunnen zijn dat over een klant veel meer gegevens zijn vastgelegd dan noodzakelijk is voor de uitvoering van de wettelijke taak. Omdat deze gevallen meestal een ingewikkelde (juridische) beoordeling vergen, worden dergelijke verzoeken behandeld door Bureau Gegevensbescherming in samenwerking met Juridische Zaken, de Archivaris en het betrokken organisatieonderdeel. Als een dergelijke verzoek in de uitvoering wordt ontvangen, moet het verzoek dan ook meteen worden doorgezonden aan Bureau Gegevensbescherming.

In het uitzonderlijke geval dat persoonsgegevens zijn verwerkt op de grondslag van toestemming van de betrokkene (zie paragraaf 4.6), moet ook aan verzoek tot verwijdering van die gegevens worden voldaan, indien de betrokkene zijn toestemming intrekt en er geen andere rechtsgrond is voor het bewaren van die gegevens.

9.4. Verzoek om de verwerking tijdelijk stil te leggen ('beperking')

Wat zegt de AVG?

Een betrokkene heeft in bepaalde gevallen het recht om te verzoeken om 'beperking van de verwerking'. Hiermee wordt bedoeld dat verzocht wordt de verwerking tijdelijk stil te leggen. De persoonsgegevens mogen dan tijdelijk niet worden gebruikt, gewist, verstrekt of anderszins verwerkt.

Artikel 18 AVG

⁷¹ Artikel 17 lid 1 onder (a) AVG

⁷² Artikel 17 lid 3 onder (d) AVG.

⁷³ Met uitzondering van de gegevens die bewaard moeten blijven en overgebracht worden naar het Nationaal Archief.

In bepaalde gevallen kan de betrokkene UWV verzoeken om de verwerking van zijn gegevens tijdelijk stil te leggen. De verwerking wordt als het ware 'bevroren'. Een verzoek hierom kan worden gedaan in de volgende gevallen:

- De betrokkene heeft om correctie van persoonsgegevens verzocht en verzoekt, in afwachting van het onderzoek van UWV m.b.t. de juistheid van die gegevens, om de verwerking te bevroren.
- De betrokkene heeft bezwaar gemaakt tegen de verwerking en verzoekt, in afwachting van het antwoord van UWV daarop, de verwerking te bevroren.
- De betrokkene heeft de persoonsgegevens nodig voor een juridische procedure of verzet zich om andere redenen tegen het wissen van gegevens, terwijl UWV de persoonsgegevens eigenlijk zou moeten wissen omdat er geen grondslag of noodzaak meer voor de verwerking is.

In paragraaf 9.6 wordt ingegaan op de uitzonderingen waarin een organisatie niet aan een verzoek van de betrokkene hoeft te voldoen. Dit moet van geval tot geval bekeken worden. Voor UWV zal in de meeste gevallen zo'n uitzondering gelden en zal niet aan een verzoek tot het stilleggen van de verwerking kunnen worden voldaan.

Verzoeken tot beperking van de verwerking worden – net als verzoeken tot vernietiging van persoonsgegevens – centraal behandeld door Bureau Gegevensbescherming in samenwerking met Juridische Zaken.

9.5. Recht om bezwaar te maken tegen de verwerking

Wat zegt de AVG?

Indien een verwerking van persoonsgegevens als grondslag heeft dat deze:

noodzakelijk is ter uitvoering van een wettelijke taak van algemeen belang, of noodzakelijk is ter behartiging van een gerechtvaardigd belang van de verwerkingsverantwoordelijke of een derde en de belangen van de betrokkene niet zwaarder wegen, kan de betrokkene bezwaar maken tegen de verwerking van zijn of haar persoonsgegevens. Het gaat hierbij vooral om situaties waarin de persoonsgegevens worden gebruikt voor profilering en geautomatiseerde besluitvorming. De organisatie die de persoonsgegevens verwerkt mag hiermee alleen doorgaan, indien deze 'dwingende gerechtvaardigde gronden' heeft voor de verwerking die zwaarder wegen dan de belangen van de betrokkene of indien deze de persoonsgegevens nodig heeft in een juridische procedure.

Artikel 21 AVG

Hoewel deze mogelijkheid vooral in het leven is geroepen voor burgers om bezwaar te kunnen maken tegen direct marketing waarbij al dan niet gebruik wordt gemaakt van klantprofielen en bedrijven te dwingen daarmee te stoppen, heeft de bepaling ook gevolgen voor UWV. Dit komt omdat ook bezwaar kan worden gemaakt tegen de verwerking van persoonsgegevens die is gebaseerd op de grondslag 'noodzakelijk voor de uitvoering van een wettelijke taak van algemeen belang'. Zoals in hoofdstuk 4 is toegelicht, is dit voor UWV de belangrijkste grondslag voor de verwerkingen.

Weliswaar zal een bezwaar tegen de verwerking van persoonsgegevens in de meeste gevallen moeten worden afgewezen op grond van het feit dat de verwerking van de persoonsgegevens noodzakelijk is om de wettelijke taken te kunnen uitvoeren, zal op een bezwaar wel gemotiveerd moeten worden geantwoord. Omdat dit een juridische aangelegenheid betreft die ook samenhangt met de Algemene wet bestuursrecht, worden dergelijke verzoeken centraal behandeld door Bureau Gegevensbescherming in samenwerking met Juridische Zaken.

9.6. Uitzonderingen op de rechten van betrokkenen

Wat zegt de AVG?

De rechten van betrokkenen zoals omschreven in dit hoofdstuk zijn niet absoluut. In bepaalde omstandigheden kunnen andere belangen zwaarder wegen waardoor er een beperking geldt voor deze rechten.

Artikel 41 UAVG

In de UAVG zijn een aantal uitzonderingen genoemd op de rechten van betrokkenen zoals hierboven omschreven. Dit betekent dat in de in artikel 41 UAVG genoemde gevallen UWV kan weigeren aan een verzoek te voldoen. De voor UWV relevante uitzonderingsgronden zijn de volgende:

- Wanneer naar de betrokkene door de Directie Handhaving of Bureau Integriteit onderzoek wordt gedaan en het verstrekken van informatie of het geven van inzage hierover dat onderzoek zou schaden.⁷⁴
- Wanneer sprake is van het delen van persoonsgegevens met politie, justitie of inlichtingendiensten en het verstrekken van informatie of het geven van inzage hierover aan de betrokkene het werk van deze diensten zou schaden.⁷⁵
- Wanneer een verzoek wordt gedaan de verwerking 'stil te leggen' (beperking, zie paragraaf 9.4) zal dit in veel gevallen strijdig zijn met het algemeen belang van de sociale zekerheid.⁷⁶ Het is van groot belang de systemen van UWV voor de uitvoering van de sociale zekerheidswetgeving accuraat te houden. Dat belang zal in de meeste gevallen groter zijn dan het belang van de betrokkene om de verwerking te beperken.

Per geval zal door UWV moeten worden afgewogen of de genoemde belangen zwaarder wegen dan de belangen van de betrokkene.

Omdat de beoordeling van verzoeken om vernietiging en beperking van de verwerking alsmede bezwaar tegen de verwerking een soms ingewikkelde afweging vergen, worden dergelijke verzoeken altijd in samenwerking met Juridische Zaken behandeld.

UWV beleidskader

- **Verzoeken om inzage en correctie van persoonsgegevens worden door de organisatieonderdelen zelf afgehandeld.**
- **Omdat het van groot belang is dat voor de medewerkers van UWV duidelijk is hoe zij moeten handelen als zij een verzoek tot inzage of correctie ontvangen, is hiervoor op DWU toegankelijke informatie beschikbaar met briefsjablonen en zijn in de handboeken procedures en instructies opgenomen.**
- **Aan de verzoeker wordt altijd binnen 5 dagen een ontvangstbevestiging gezonden.**
- **Gestreefd wordt dergelijke verzoeken binnen de voorgeschreven termijn van één maand af te handelen. Als dit niet mogelijk is, wordt de betrokkene tenminste binnen een maand na ontvangst van zijn verzoek in kennis gesteld van de behandeling daarvan en de termijn waarbinnen daaraan zal worden gehoor gegeven.**
- **Wanneer verzoeken onduidelijk of complex zijn of niet aan een verzoek kan worden voldaan, wordt met de betrokkene contact opgenomen om uitleg te vragen of te geven.**
- **Verzoeken tot verwijdering van persoonsgegevens, beperking van de verwerking of wanneer bezwaar wordt gemaakt tegen de verwerking, zijn vaak complex. Daarom wordt in dergelijke gevallen centraal afgehandeld door Bureau Gegevensbescherming en Juridische Zaken.**

⁷⁴ Artikel 41 lid 1 sub (h) AVG.

⁷⁵ Artikel 41 lid 1 sub (a) AVG.

⁷⁶ Artikel 41 lid 1 sub (e) AVG.

-
- Er vindt registratie plaats (ten behoeve van de FG en AP) van de ontvangen verzoeken, de wijze van afhandeling en de termijn waarbinnen dit is gebeurd.

10. Functionaris Gegevensbescherming (FG)

Wat zegt de AVG?

Op grond van de AVG zijn alle overheidsinstanties verplicht om een FG aan te wijzen die voor de organisatie ten minste de volgende taken vervult:

- het informeren en adviseren van leiding en medewerkers van UWV over hun verplichtingen onder de AVG,
- het toezien op de naleving van AVG binnen UWV,
- het adviseren en toezien op de uitvoering van GEBs,
- centraal aanspreekpunt zijn voor de Autoriteit Persoonsgegevens en met deze samenwerken,
- formeel aanspreekpunt zijn voor betrokkenen (o.a. formele klachtenafhandeling).

De AVG schrijft voor dat de FG een onafhankelijke positie heeft en direct rapporteert aan het hoogst leidinggevend niveau. Die onafhankelijkheid betekent niet dat de FG geen aanvullende taken mag uitvoeren, maar wel dat deze niet mogen leiden tot een belangenconflict. De FG moet van voldoende middelen zijn voorzien om zijn taken goed te kunnen uitvoeren.

Artikelen 37 lid 1, 38 lid 2 en 3 en artikel 39 AVG

De FG heeft een belangrijke taak om een organisatie te helpen voldoen aan de eisen die de AVG stelt. De FG doet dat in de eerste plaats door de Raad van Bestuur, management en medewerkers van de organisatie te informeren en te adviseren over de verplichtingen die voortvloeien uit de AVG. Daarnaast heeft de FG ook een toetsende rol en ziet hij als interne toezichthouder toe op de naleving van de AVG binnen de verschillende organisatieonderdelen. Hij kan bijvoorbeeld intern onderzoek doen naar een bepaalde verwerking. Om deze rollen goed te kunnen vervullen dient de FG te beschikken over voldoende middelen en dient hij een zekere onafhankelijkheid te hebben. Hij mag niet tevens belast zijn met de verantwoordelijkheid voor de uitvoering van het primaire proces en voor de gegevensverwerkingen binnen UWV die daarmee verband houden, omdat dat tot een belangenconflict zou kunnen leiden. Maar tegelijkertijd moet hij ook niet op te grote afstand van de organisatie komen te staan. Door voor de medewerkers toegankelijk te zijn en bekend te zijn met de bedrijfsvoering van UWV kan de FG zijn adviezen beter afstemmen op de specifieke situatie van UWV.

De FG van UWV is gepositioneerd binnen de Directie Bestuurszaken. Hier is zijn onafhankelijkheid ten aanzien van de organisatieonderdelen geborgd, heeft hij directe toegang tot (de voorzitter van) de Raad van Bestuur en heeft hij voldoende aansluiting op de rest van de organisatie om gericht te kunnen adviseren over het (gaan) voldoen aan de verplichtingen van de AVG. De FG wordt bij zijn taken ondersteund door medewerkers van het Bureau Gegevensbescherming. Hij is tevens hoofd van dit bureau.

Hoewel BKWI bestuurlijk een aparte positie binnen UWV heeft, is BKWI formeel wel een onderdeel van UWV. De FG van UWV is daarom ook de FG van BKWI en voor de Autoriteit Persoonsgegevens het aanspreekpunt voor BKWI.

De FG onderhoudt contacten met de Autoriteit Persoonsgegevens. Wanneer de AP echter in het kader van een (handhavings)onderzoek UWV om inlichtingen verzoekt, verloopt de communicatie tussen UWV en de AP in principe via JZ. Hierdoor kan de FG zijn onafhankelijke positie behouden en kan JZ zijn rol als bedrijfsjurist van UWV vervullen.

Bureau Gegevensbescherming

Zoals gezegd ondersteunen de medewerkers van Bureau Gegevensbescherming de Functionaris Gegevensbescherming bij zijn taken. Het gaat bijvoorbeeld om de beoordeling van GEBs, het beantwoorden van correspondentie en klachten en het uitvoeren van onderzoek. Daarnaast is ook het beheer over een aantal centrale AVG-processen bij het Bureau Gegevensbescherming belegd. Het gaat om de volgende processen:

- Onderhoud van het beleidskader privacy;
- Onderhoud van het register van verwerkingen;
- Onderhoud van de privacyverklaring voor klanten;

-
- Beheer van het proces voor registratie en meldingen van beveiligingsincidenten en datalekken en het melden van datalekken aan de Autoriteit Persoonsgegevens;
 - Beheer van het proces voor verzoeken tot inzage en correctie van persoonsgegevens;
 - Beheer van het proces voor en de afhandeling van verzoeken tot vernietiging van persoonsgegevens, beperking van en bezwaar tegen de verwerking van persoonsgegevens;
 - Beheer van het GEB-proces.

11. Instrumentarium en specifieke procedures

Naast de procedures die direct verband houden met de rechten van betrokkenen (zie hoofdstuk 10), zijn er nog enkele andere concrete procedures waar de medewerkers van UWV een rol in spelen. Deze worden in dit hoofdstuk kort beschreven.

11.1. Gegevensbeschermingseffectbeoordeling (GEB)

Wat zegt de AVG?

Organisaties moeten een gegevensbeschermingseffectbeoordeling (GEB) uitvoeren indien een voorgenomen verwerking van persoonsgegevens waarschijnlijk een hoog risico voor de rechten en vrijheden van de betrokkene met zich meebrengt. De Functionaris gegevensbescherming brengt advies uit over (de noodzaak van) de GEB en ziet toe op de uitvoering van GEBs.

Als de uitkomst van een GEB een hoog risico voor de privacy van betrokkene laat zien terwijl mitigerende maatregelen niet afdoende zijn, moet de voorgenomen verwerking voor advies aan de Autoriteit Persoonsgegevens worden voorgelegd.

Artikel 35 AVG

De GEB richt zich op het identificeren en beheersen van privacyrisico's die betrekking hebben op de verwerking van persoonsgegevens binnen UWV. Een GEB wordt uitgewerkt in een GEB-rapport met 4 onderdelen:

- beschrijving van de kenmerken van de (beoogde) gegevensverwerking;
- beoordeling van de rechtmatigheid (inclusief de grondslag) van de gegevensverwerking;
- de in kaart gebrachte privacyrisico's voor de betrokkenen; en
- de voorgenomen maatregelen om de privacyrisico's te mitigeren.

Binnen UWV is een GEB-proces vastgesteld met procesafspraken en ondersteunende sjablonen.. Het GEB-proces bestaat uit het uitvoeren van een GEB-check om te beoordelen of een GEB noodzakelijk is en het daadwerkelijk uitwerken van het GEB-rapport. De procesbeschrijving en de sjablonen zijn te raadplegen op de GEB-pagina op DWU. Hier is ook een uitgebreide Handreiking GEB-proces gepubliceerd die organisatieonderdelen ondersteunt bij het uitvoeren van een GEB. Zie voor de precieze locatie van deze stukken bijlage I.

Binnen UWV geldt de afspraak dat bij ieder nieuw project en bij wijzigingen met een substantiële impact op het privacyrisico minimaal een GEB-check wordt uitgevoerd en – afhankelijk van de uitkomst van de GEB-check – een volledige GEB. Hierbij wordt de procedure gevolgd en worden de sjablonen gebruikt zoals deze op DWU beschikbaar zijn gesteld.

Aanbevolen wordt om bij het uitvoeren van een GEB ook inhoudelijke experts van buiten het eigen organisatieonderdeel te betrekken. Zo kunnen de privacy-juristen van JZ adviseren over de juridische kwalificaties van de voorgenomen verwerking in de GEB en de adviseurs van CISO-office een bijdrage leveren aan de identificatie van risico's en de mogelijke mitigerende maatregelen.

De BSO heeft een belangrijke kwaliteitsbewakende functie in het GEB-proces. Voordat een GEB-check of GEB-rapport aan de FG wordt gezonden, dient dit te worden beoordeeld door de BSO die zijn oordeel ook in het rapport vastlegt. De BSO dient erop toe te zien dat alleen rapporten die van voldoende kwaliteit zijn, worden doorgezonden aan de FG.

De FG beoordeelt vervolgens de GEB-checks en GEB-rapporten in samenspraak met de adviseurs van Bureau Gegevensbescherming. Zij komen iedere week bijeen (in de zogenoemde 'GEB-board'). De FG verstuurt op basis

van deze bespreking zijn oordeel aan de indiener van de GEB(-check) en de BSO van het desbetreffende organisatieonderdeel.

Voorafgaande raadpleging van Autoriteit Persoonsgegevens

Als de uitkomst van een GEB tot de conclusie leidt dat het risico voor de betrokkene van de voorgenomen verwerking hoog is, doordat niet voldoende mitigerende maatregelen worden getroffen, is UWV verplicht de voorgenomen verwerking voor advies voor te leggen aan de Autoriteit Persoonsgegevens. Dit is vastgelegd in artikel 36 AVG.

Wanneer zich zo'n situatie voordoet, vindt overleg plaats tussen de FG, Bureau Gegevensbescherming, Juridische Zaken en de desbetreffende divisie of directie.

Op de website van de Autoriteit Persoonsgegevens is de procedure beschreven die in dergelijke gevallen moet worden gevolgd. Daar is ook het formulier "Verzoek voorafgaande raadpleging" te downloaden dat hierbij moet worden gebruikt.

11.2. Melden van beveiligingsincidenten en datalekken

Wat zegt de AVG?

Op het moment dat een organisatie kennis heeft genomen van het feit dat zich een datalek heeft voorgedaan, moet het datalek onverwijld, maar uiterlijk binnen 72 uur aan de [Autoriteit Persoonsgegevens](#) (AP) worden gemeld, tenzij onwaarschijnlijk is dat het datalek een risico vormt voor de rechten en vrijheden van de betrokkene. In bepaalde gevallen moet het datalek ook aan de [betrokkene zelf](#) (degene van wie persoonsgegevens zijn 'gelekt') worden gemeld, namelijk wanneer het risico voor de betrokkene waarschijnlijk hoog is.

Artikel 33 en 34 AVG

Een datalek is een inbreuk op of gebrek in de technische of organisatorische beveiliging van persoonsgegevens waardoor – zonder dat dit de bedoeling is – persoonsgegevens zijn vernietigd, gewijzigd of verloren zijn gegaan, of onbevoegde verstrekking of toegang tot persoonsgegevens heeft plaatsgevonden. Bij een datalek kan het dus gaan om een inbreuk op de beschikbaarheid (onbevoegde vernietiging of verlies van persoonsgegevens), op de integriteit (onbevoegde wijziging van persoonsgegevens) of op de vertrouwelijkheid (onbevoegde verstrekking van of toegang tot persoonsgegevens).

Om te kunnen beoordelen of sprake is van een datalek moet ieder beveiligingsincident direct worden gemeld via het Meldproces beveiligingsincident met persoonsgegevens ('datalekken') en het bijbehorende meldformulier dat op DWU beschikbaar is voor alle medewerkers. Het direct melden is van belang om eventuele schade als gevolg van het incident te kunnen beperken en om de termijnen voor het melden aan de Autoriteit Persoonsgegevens te kunnen halen. Na de melding beoordeelt Bureau Gegevensbescherming of het beveiligingsincident ook als datalek moet worden gekwalificeerd en of dit aan de AP en mogelijk ook aan de betrokkene moet worden gemeld. In complexe gevallen wordt hierbij Juridische Zaken geconsulteerd. Als het beveiligingsincident als datalek wordt aangemerkt dat aan de Autoriteit Persoonsgegevens moet worden gemeld, dient dit binnen 72 uur na vaststelling dat er sprake is van een datalek te gebeuren. Ook wordt beoordeeld of de betrokkene van het datalek in kennis moet worden gesteld. Dit is het geval wanneer het datalek waarschijnlijk een hoog risico voor de betrokkene met zich meebrengt.

Voorbeelden van datalekken zijn:

- brieven die aan de verkeerde persoon zijn gestuurd en vervolgens zijn geopend;
- een bestand met persoonsgegevens dat in een werkmap wordt geplaatst en niet voor de betrokkene bedoeld is;
- een bestand met persoonsgegevens dat per e-mail wordt meegezonden naar een geadresseerde voor wie de gegevens niet bedoeld zijn;
- een hacker die de systemen van UWV binnendringt en persoonsgegevens wijzigt, vernietigt of daarvan kennisneemt.

Bij een mogelijk datalek moet allereerst worden beoordeeld of er persoonsgegevens bij het incident waren betrokken. De inbraak in een kantoorpand waarbij geen persoonsgegevens zijn verdwenen is een voorbeeld van een incident dat geen datalek is. Een ander voorbeeld van een datalek dat in principe niet aan de AP hoeft te worden gemeld is het verliezen van een door UWV beschikbaar gestelde laptop of telefoon. Aangezien deze middelen op voldoende niveau versleuteld zijn, hoeft het verlies hiervan niet als datalek aan de AP te worden gemeld. Uiteraard moet dit wel worden gemeld, ook aan Bureau Integriteit. Op DWU is een pagina beschikbaar met informatie over wat te doen in geval van verlies of diefstal van een eigendom op de werkplek of daarbuiten.

De procedures die moeten worden gevolgd in geval van een beveiligingsincident of mogelijk datalek zijn uitgewerkt in instructies voor de medewerkers en te vinden op DWU. Zie hiervoor de pagina 'Melden van beveiligingsincidenten en datalekken' (zie bijlage).

In het proces dat is opgesteld voor het melden van datalekken heeft het IB&P-team van het desbetreffende organisatieonderdeel een coördinerende rol. Deze vormt de schakel tussen de centrale partijen (BIS-team van de Servicedesk IV en Bureau Gegevensbescherming) enerzijds en het organisatieonderdeel anderzijds.

Datalekken zijn in veel gevallen het gevolg van menselijke fouten. Het is van groot belang dat een vermoeden van een datalek zo snel mogelijk gemeld wordt. In veel gevallen kan daarmee de schade worden beperkt (een werkmapbericht kan bijvoorbeeld worden teruggehaald via de servicedesk IV).

Om datalekken te voorkomen is het belangrijk dat:

- medewerkers goed geïnstrueerd zijn en zich bewust zijn van de risico's;
- voor risicovolle processen het vier-ogen principe geldt, dat wil zeggen dat een tweede persoon bepaalde handelingen van de eerste persoon controleert voordat de actie wordt uitgevoerd;
- nieuwe en bestaande systemen en processen zo worden ingericht dat de kans op een datalek zo klein als mogelijk wordt (privacy by design/default).

Daarnaast is het voor een goed proces rond het melden van datalekken van belang dat:

- een veilige omgeving wordt gecreëerd zodat datalekken snel worden gemeld; en
- medewerkers de procedures kennen die hiervoor gelden voor het tijdig melden van datalekken.

Ten slotte is het van belang dat organisatieonderdelen datalekken goed evalueren. Een datalek duidt op een risico in een bepaald proces. Het is van belang om te beoordelen of dit al een bekend risico was en of er voldoende mitigerende maatregelen zijn getroffen. Zeker wanneer een bepaald datalek vaker voorkomt is het aan te raden dit verder te onderzoeken en de bevindingen vast te leggen. De toezichthouder kan hier ook om vragen.

Calamiteitenplan datalekken

Binnen UWV is een calamiteitenplan ontwikkeld dat tot doel heeft om duidelijkheid te geven over welke stappen kunnen worden ondernomen wanneer zich een impactvol datalek heeft voorgedaan. Het calamiteitenplan treedt in werking als een datalek als impactvol wordt aangemerkt, namelijk wanneer het datalek wordt opgeschaald van incident naar calamiteit. De directeur (of een door hem of haar gemandateerde) van het organisatieonderdeel waar het datalek zich voordoet, neemt het besluit om het calamiteitenplan in werking te laten treden en op te schalen van incident naar calamiteit. Dit is van belang omdat het opstarten van het calamiteitenplan ook gevolgen heeft voor de inzet van capaciteit en prioritering van werkzaamheden. De BSO heeft hierbij een belangrijke signalerende en adviserende functie richting de directeur/gemandateerde.

11.3. Schadeclaim bij datalek

Wat zegt de AVG?

Als een persoon materiële of immateriële schade heeft geleden als gevolg van een datalek, kan hij of zij recht hebben op een schadevergoeding.

Artikel 82 AVG

Een betrokkene kan UWV aansprakelijk stellen voor materiële of immateriële schade die hij of zij heeft geleden als gevolg van een datalek. Onder bepaalde gevallen is UWV verplicht die schade geheel of gedeeltelijk te vergoeden. Dit vergt een goede juridische beoordeling. Daarom worden verzoeken tot schadevergoeding als gevolg van een datalek centraal behandeld door Juridische Zaken. Als een medewerker een dergelijk verzoek tot schadevergoeding (schadeclaim) ontvangt, wordt dit verzoek doorgezonden aan Juridische Zaken. De betrokkene wordt hiervan in kennis gesteld.

11.4. Melding wijzigingen register van verwerkingen

In paragraaf 8.2 is ingegaan op het register van verwerkingen dat UWV bijhoudt. Dit register is te vinden op DWU. Het spreekt voor zich dat dit register een actuele status moet weergeven. Daarom is binnen UWV een procedure opgesteld om wijzigingen door te geven die in dit register moeten worden verwerkt. Deze procedure alsmede het formulier dat moet worden gebruikt om wijzigingen door te geven, is eveneens te vinden op DWU onder de naam 'Mutatie register van verwerkingen van persoonsgegevens'. Zie ook bijlage I.

UWV beleidskader

Gegevensbeschermingseffectbeoordeling (GEB)

- UWV heeft een procedure en sjablonen voor het GEB-proces. Deze zijn gepubliceerd op DWU.
- De BSO vervult een kwaliteitsbewakende rol en ziet erop toe dat alleen GEBs van voldoende kwaliteit worden doorgestuurd aan de FG.
- Het verdient aanbeveling om experts, zoals JZ of CISO, te betrekken bij het uitvoeren van een GEB.
- Voor ieder nieuw project en voor wijzigingen met een substantiële impact op de bestaande verwerkingen wordt een GEB-check uitgevoerd en, afhankelijk van de uitkomst van de GEB-check, een volledige GEB. Hierbij wordt de procedure en de sjablonen zoals beschikbaar gesteld op DWU gevolgd.

Meldproces datalekken

- UWV heeft een procedure voor het melden van (mogelijke) datalekken. Deze is gepubliceerd op DWU.
- Ieder organisatieonderdeel zorgt ervoor dat zijn medewerkers goed zijn geïnstrueerd over de risico's op datalekken en de wijze waarop deze kunnen worden voorkomen.
- Ook zorgt ieder organisatieonderdeel ervoor dat de medewerkers en managers op de hoogte zijn van de procedures die moeten worden gevolgd als er sprake is van een (vermoeden van) een datalek.
- Het IB&P-team van het desbetreffende organisatieonderdeel heeft in dit proces een coördinerende rol en is het aanspreekpunt voor de centrale partijen (BIS-team en Bureau Gegevensbescherming).

- Er is een Calamiteitenplan Datalekken dat een stappenplan bevat dat kan worden gevolgd in geval van een impactvol datalek.

Verzoek om schadevergoeding

- In bepaalde gevallen is UWV verplicht schade te vergoeden die een betrokkene heeft geleden als gevolg van een datalek. Omdat dit een complexe juridische beoordeling vergt, worden dergelijke verzoeken (schadeclaims) centraal behandeld door Juridische Zaken.
- Indien een medewerker een schriftelijk verzoek tot schadevergoeding ontvangt, wordt dat verzoek doorgestuurd naar Juridische Zaken. De persoon die het verzoek heeft ingediend, wordt hiervan op de hoogte gesteld.

Melding wijziging register van verwerkingen

- UWV heeft een procedure en formulier voor het aanvullen of wijzigen van het register van verwerkingen.
- Iedere proceseigenaar is ervoor verantwoordelijk om nieuwe verwerkingen of wijzigingen met betrekking tot bestaande verwerkingen door te geven aan IB&P BZ. Hiervoor worden de op DWU beschreven procedure gevolgd en het formulier 'mutatie register van verwerkingen van persoonsgegevens' gebruikt.

Lijst van afkortingen

AP	Autoriteit Persoonsgegevens
AVG	Algemene verordening gegevensbescherming
BZ	Bestuurszaken
BIO	Baseline Informatiebeveiliging Overheid
BIR	Baseline Informatiebeveiliging Rijksoverheid
CISO	Chief Information Security Officer
C-ICT	Concern ICT
DWU	Digitale Werkplek
DHH	Directie Handhaving
EER	Europees Economische Ruimte (lidstaten EU + Noorwegen, IJsland en Liechtenstein)
FG	Functionaris Gegevensbescherming
GEB	Gegevensbeschermingseffectrapportage
IB&P	Informatiebeveiliging en privacy
JZ	Juridische Zaken
SMZ	Divisie Sociaal Medische Zaken
UAVG	Uitvoeringswet Algemene verordening gegevensbescherming
Wbp	Wet bescherming persoonsgegevens (de voorloper van de AVG)

Bijlage I Overzicht relevante beleidsstukken en instructies

Security & Privacy by Design and Default

- Security & Privacy by Design and Default
https://samenwerken.sharepoint.uwv.nl/sites/DWU/ConcernICT/IBenP/IBenP%20Themapagina%27s/_layouts/15/start.aspx#/SitePages/Privacy%20en%20Security%20by%20design.aspx

Anonimiseren en pseudonimiseren

- UWV Richtlijn Data Anonimisering en pseudonimisering (versie 1.1, 27-07-2018)
<https://samenwerken.sharepoint.uwv.nl/sites/DWU/ConcernICT/Paginas/Overzicht-IBenP-beleid--en-richtlijnen.aspx>

Gezondheidsgegevens

- Richtlijn beheer gegevens vallend onder het medisch beroepsgeheim van de verzekeringsarts
<https://digitalewerkplek.sharepoint.uwv.nl/documentcenter/Documenten/Medezeggenschap/Beleidsdocument/Richtlijn+BMG+versie+maart+2010.pdf>
Deze richtlijn wordt in 2021 vervangen door de *UWV Richtlijn Omgaan met Gezondheidsgegevens*
- Regeling beheer en verkeer medische gegevens B&B
<https://digitalewerkplek.sharepoint.uwv.nl/werkprocessen/Paginas/Beheerverkeermedischegegevens.aspx>
- KNMG-Richtlijn Omgaan met medische gegevens
<https://www.knmg.nl/advies-richtlijnen/knmg-publicaties/omgaan-met-medische-gegevens.htm>

Burgerservicenummer

- Handleiding gebruik BSN UWV
https://digitalewerkplek.sharepoint.uwv.nl/documentcenter/Documenten/Bestuurszaken/Team%20IBP%20BZ/Beleidsdocument/Handleiding_gebruik_BSN_UWV.docx

Cameratoezicht

- Videocameratoezichtprotocol versie 1.0 vastgesteld op 31-7-2019 door het MT Huisvesting van Facilitair Bedrijf.
https://digitalewerkplek.sharepoint.uwv.nl/documentcenter/Documenten/Facilitair%20Bedrijf/Beleidsdocument/Videocameratoezicht_protocol.pdf

Verstrekking van persoonsgegevens aan derden

- Instructie gegevensverstrekking aan derden (IGAD)
<http://handboeken.info.uwv.nl/index.htm?handboek=23821&daversie=actueel&dadocr=d20080108t11410437>
- Intake informatieverzoek
<http://handboeken.info.uwv.nl/index.htm?dahandboek=ikwinf&dadocr=d20120803t135731233&daversie=actueel>

Gebruik open bronnen

- Protocol Internetonderzoek Directie Handhaving UWV, datum onbekend, publicatie op DWU laatst bijgewerkt op 15-5-2019
<https://digitalewerkplek.sharepoint.uwv.nl/documentcenter/Documenten/Handhaving/Beleidsdocument/herschreven%20protocol%20internet%20onderzoek%20DHH%201.1.pdf> of via:
<https://digitalewerkplek.sharepoint.uwv.nl/uwv/organisatieonderdelen/Handhaving/Paginas/WerkinstructieseninformatieDirectieHandhaving.aspx>
- Onderzoeksprotocol Bureau Integriteit UWV
<https://digitalewerkplek.sharepoint.uwv.nl/documentcenter/Documenten/Medezeggenschap/Vergaderinformatie/2017/Onderzoeksprotocol%20febr%202021.pdf>
- NVP sollicitatiecode
<https://nvp-plaza.nl/sollicitatiecode>

Analyse, profilering en geautomatiseerde besluitvorming

- Normenkader dataanalyseomgevingen, dd. 1 december 2020
<https://digitalewerkplek.sharepoint.uwv.nl/documentcenter/Documenten/Gegevensdiensten/Beleidsdocument/UWV%20Inrichtingskader%20versie%202.0%20def.docx>
- Visie Datagedreven UWV, kaderstelling, november 2020

<https://digitalewerkplek.sharepoint.uwv.nl/uwv/organisatieonderdelen/Paginas/DataOfficeUWVProductenenKaders.aspx>

- Visie Datagedreven UWV, Strategische vraagstukken, november 2020

<https://digitalewerkplek.sharepoint.uwv.nl/uwv/organisatieonderdelen/Paginas/DataOfficeUWVProductenenKaders.aspx>

Classificatie en beveiliging van persoonsgegevens

- BIO
<https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/informatieveiligheid/kaders-voor-informatieveiligheid/baseline-informatiebeveiliging-overheid/>
- BIV-classificatiedocument 2.0
https://digitalewerkplek.sharepoint.uwv.nl/documentcenter/Documenten/Bestuurszaken/Team%20IBP%20BZ/Beleidsdocument/UWV_BZ_BIV_Classificatie.docx
- Handreiking betrouwbaarheidsniveaus voor digitale dienstverlening
<https://www.forumstandaardisatie.nl/thema/handreiking-betrouwbaarheidsniveaus>
- Autorisatiebeheer
<https://digitalewerkplek.sharepoint.uwv.nl/services/management/Paginas/AutorisatiebeheerbijHRM.aspx>

Bewaren, archiveren, vernietigen

- Selectielijst UWV
<https://digitalewerkplek.sharepoint.uwv.nl/documentcenter/Documenten/Facilitair%20Bedrijf/Beleidsdocument/Notitie-Bewaarregels-en-Bewaartermijnen-selectielijst-UWV.pdf>
- Regeling Archiefbeheer UWV
<http://contentregister.info.uwv.nl/Bestanden/FI14014885.pdf>
- Notitie Bewaarregels en Bewaartermijnen
<https://digitalewerkplek.sharepoint.uwv.nl/documentcenter/Documenten/Facilitair%20Bedrijf/Beleidsdocument/Notitie-Bewaarregels-en-Bewaartermijnen-selectielijst-UWV.pdf>
- Data life cycle management
<https://digitalewerkplek.sharepoint.uwv.nl/uwv/organisatieonderdelen/Paginas/DataOfficeUWVProductenenKaders.aspx>

Transparantie

- Privacyverklaring voor klanten (klantcommunicatie)
<https://www.uwv.nl/privacy/index.aspx>
- Privacyverklaring voor evenementen
<https://www.uwv.nl/privacy/overige-privacyverklaringen/index.aspx>
- Privacyverklaring voor werkgevers
<https://www.uwv.nl/privacy/overige-privacyverklaringen/index.aspx>
- Privacyverklaring voor medewerkers
<https://digitalewerkplek.sharepoint.uwv.nl/documentcenter/Documenten/HRM/Communicatiemiddel/Privacyverklaring%20medewerkers%20UWV%202021.210.pdf>
- Register van verwerkingen
<https://digitalewerkplek.sharepoint.uwv.nl/uwv/organisatieonderdelen/Bestuurszaken/Paginas/Registerverwerkingenvanpersoonsgegevens.aspx>
- Mutatieverzoek register van verwerkingen van persoonsgegevens
<https://digitalewerkplek.sharepoint.uwv.nl/uwv/organisatieonderdelen/Bestuurszaken/Paginas/Registerverwerkingenvanpersoonsgegevens.aspx>

Rechten van betrokkenen

- DWU-pagina Verzoeken tot inzage en correctie van persoonsgegevens

<https://digitalewerkplek.sharepoint.uwv.nl/uwv/organisatieonderdelen/Bestuurszaken/Paginas/Verzoekentotinzageofcorrectievanpersoonsgegevens.aspx>

- Regeling inzake- en correctierecht UWV 2018

<https://wetten.overheid.nl/BWBR0040934/2018-05-25>

- Handboek 'proces informatie verstrekken'

<https://digitalewerkplek.sharepoint.uwv.nl/werkprocessen/kennispoorten/Paginas/kennispoort-informatieverstrekking.aspx>

- Handboek 'behandelen verzoek om correctie'

<http://handboeken.info.uwv.nl/index.htm?dahandboek=ikwinf&dadocnr=d20120507t083348535&daversie=actueel>

Instrumenten en procedures

- Gegevensbeschermingseffectbeoordeling (GEB)

<https://digitalewerkplek.sharepoint.uwv.nl/uwv/organisatieonderdelen/Bestuurszaken/Paginas/GegevensbeschermingseffectbeoordelingGEB.aspx>

- Melden van beveiligingsincidenten en datalekken + Calamiteitenplan datalekken

<https://digitalewerkplek.sharepoint.uwv.nl/uwv/organisatieonderdelen/Bestuurszaken/Paginas/Meldenvanbeveiligingsincidentenendatalekken.aspx>

- DWU-pagina Wat te doen bij diefstal of vermissing?

<https://digitalewerkplek.sharepoint.uwv.nl/services/werkplek/Paginas/vermissingdiefstal.aspx>

- Calamiteitenplan datalekken (stappenplan voor het optreden bij een impactvol datalek)

<https://digitalewerkplek.sharepoint.uwv.nl/uwv/organisatieonderdelen/Bestuurszaken/Paginas/Meldenvanbeveiligingsincidentenendatalekken.aspx>

Overig

- Gouden regels voor het veilig omgaan met informatie

https://digitalewerkplek.sharepoint.uwv.nl/documentcenter/Documenten/Bestuurszaken/Team%20IBP%20BZ/Bestuurlijk%20document/UWV_gouden_regels.pdf

- Beveiligings- en Verwerkersovereenkomsten

<https://samenwerken.sharepoint.uwv.nl/sites/DWU/ConcernICT/Paginas/Overzicht-IBenP-beleid--en-richtlijnen.aspx>

- Gedragscode UWV Vertrouwen en verantwoordelijkheid

<https://digitalewerkplek.sharepoint.uwv.nl/nieuws/Paginas/GedragscodeUWVaangepastaanactuelesituatie.aspx>

- Uitvoeringsbeleid Adressen op burgerservicenummer niveau

<https://digitalewerkplek.sharepoint.uwv.nl/documentcenter/Documenten/Gegevensdiensten/Beleidsdocument/Uitvoeringsbeleid%20Adressen%20op%20BSN%20niveau%20v2.0.pdf>

Dit beleidskader is een uitgave van:

Bureau Gegevensbescherming i.s.m. Juridische Zaken

Inlichtingen

ibpbz@uwv.nl