Testen met persoonsgegevens buiten de productieomgeving

Een CIP-bewerking van:
"*Persoonsgegevens buiten de productieomgeving*" v.1.9,
Marcel Koers, UWV, 18 maart 2013.

Bewerking en redactie: Ruud de Bruijn
Centrum voor Informatiebeveiliging en Privacybescherming
3 juni 2013 : versie 1.0

6 augustus 2013 : versie 1.1
21 oktober 2013 : versie 1.2
4 april 2014 : versie 1.2 licentiemelding toegevoegd

Inhoud

1 Inleiding

1.1 Doel van dit document

Het doel van dit document is om beveiligingsgerelateerde richtlijnen te geven voor het gebruik van persoonsgegevens in testsituaties buiten de productieomgeving. Het document is in lijn met de gangbare algemene baselines, normenkaders en best practices, met name de ISO 27xxx normen, de Code voor Informatiebeveiliging, en de BIR-TNK voor zover van toepassing[1].

1.2 Herkomst en status

Dit document is een bewerking van: Marcel Koers *Persoonsgegevens buiten de productieomgeving*, v.1.9, UWV, 18 maart 2013, op basis van een review door deelnemers uit het veld van CIP.
Het origineel is een UWV-intern beleidsstuk. Deze publicatie heeft die status natuurlijk niet en is dan ook ontdaan van specifieke verwijzingen naar UWV-beleid, tenzij het passages betreft die als voorbeeld of illustratie kunnen dienen.

Met het doel informatie-uitwisseling en kennisdeling te bevorderen, wil CIP onder andere 'good practices' ter beschikking stellen. Dit kunnen praktijkvoorbeelden zijn, handreikingen voor beleid, beschrijvingen van de stand van zaken in bepaalde ontwikkelingen, en dergelijke. De herkomst is van oorsprong een reflectie op een onderwerp door mensen in de CIP-kring, maar kunnen ook notities zijn uit de praktijk van de CIP-organisaties die zonder verder commentaar worden gepubliceerd.
De kern is dat de bijdragen altijd zijn gebaseerd op de expertise van de deelnemende reviewers en/of het idee dat wat in één organisatie goed werkt, ook voor andere organisaties nuttig zou kunnen zijn. Soms is het resultaat dus de uitkomst van een groepsproces en in andere gevallen wordt iets 'as is' ter kennisneming of overname aangeboden.

De CIP-documenten zijn voor iedereen vrij te gebruiken en te becommentariëren. Zij hebben geen ander doel dan kennisoverdracht en reflecteren niet noodzakelijk de opvattingen van alle contribuanten, CIP-deelnemers en/of alle CIP-partijen. Publicatie vindt plaats op zowel de openbare website www.cip-overheid.nl als het besloten www.cip-pleio.nl.

Om extra duidelijkheid te scheppen labelt CIP de documenten volgens deze indeling:

1. Individuele praktijk: een toepassing bij een van de organisaties die werkt, als handreiking voor hergebruik binnen geïnteresseerde organisaties.
2. Becommentarieerde praktijk: een door meerdere professionals veralgemeniseerde praktijk als handreiking voor hergebruik binnen geïnteresseerde organisaties.
3. Gecommitteerde praktijk: een namens meerdere in CIP samenwerkende organisaties onderschreven praktijk, als sterk advies voor hergebruik bij alle organisaties binnen de uitvoerende overheid.
4. Verplichtende praktijk: een praktijk die door de in CIP samenwerkende organisaties is bekrachtigd als basis voor zelfregulering binnen deze kring en met een sterk advies om dat voor de gehele overheidslaag van de uitvoering toe te passen.

Een individuele praktijk is al bruikbaar nadat een individuele organisatie die aanreikt. Een becommentarieerde praktijk ondergaat eerst een reviewslag binnen een CIP-domeingroep en/of

[1] BIR-TNK is specifiek voor de Rijksoverheid: De nieuwe Baseline Informatiebeveiliging Rijksdienst (BIR) vervangt alle departementale en interdepartementale baselines op gebied van informatiebeveiliging en bestaat uit een tactisch normenkader (TNK) en een operationele baseline (OB). Het tactische normenkader is verplicht (comply or explain). De operationele baseline is niet verplicht, het is een best practice . Bron: http://www.gertkoolwijk.nl/de-baseline-informatiebeveiliging-rijksdienst-bir

door de CIP-Leesgroep. Een praktijk is pas gecommitteerd of verplichtend als bestuurders daarvoor hebben gekozen. Dat zijn geen inherente eigenschappen van CIP-documenten.

Op www.cip-overheid.nl kunt u een uitgebreidere versie van dit protocol raadplegen: "De totstandkoming en status van CIP-publicaties v1_1.doc".

Deze publicatie valt in de categorie 2.

1.3 Verwerking van commentaar

De reviewers zijn het onderling niet eens over een principiële kwestie: mag je onder voorwaarden productiegegevens gebruiken voor het testen van applicatiefunctionaliteit, of is dat nooit toegestaan?
In dit stuk wordt gekozen voor de opvatting van de meerderheid van de reviewers, namelijk dat testen met persoonsgegevens is toegestaan onder voorwaarden en indien dat – in redelijkheid – de enige manier is om voldoende garanties uit de testen te kunnen verkrijgen. De voornaamste legitimatie hiervoor is gelegen in de meer of minder expliciet geformuleerde openingen die de WBP, de Richtlijnen van het CBP en de BIR-TNK daarvoor bieden[2].

Een tweede verschil van opvatting betreft het karakter van dit document: moet het een beleids-stuk zijn met de principes op basis waarvan de uitvoering moet worden ingericht, of moet het juist praktische aanwijzingen bevatten voor de uitvoering? In dit stuk wordt aan beide aspecten aandacht besteed, met dien verstande dat tevens zoveel mogelijk wordt verwezen naar reeds bestaand en beproefd materiaal, zoals in 1.1 reeds is aangegeven.

2 Reikwijdte en enkele definities

2.1 Testen met persoonsgegevens

De eisen voor omgaan met persoonsgegevens van derden kennen een wettelijke basis.
De Wbp verstaat onder de *Verwerking van persoonsgegevens: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.*

Deze notitie betreft specifiek het gebruik van (elektronische) gegevensbestanden voor het testen van (elektronische) gegevensverwerking, hierna 'test' te noemen, met als bijzonderheid dat de gebruikte gegevensbestanden persoonsgegevens bevatten.[3] [4]

---

[2] WBP en CBP leggen de verantwoordelijkheid voor zorgvuldig handelen bij de verantwoordelijke (organisatie). BIR TNK is daarin wat explicieter: par. 12.4.2. (…) *Het gebruik van kopieën van operationele databases voor testgegevens wordt vermeden. Indien toch noodzakelijk, worden de gegevens zoveel mogelijk geanonimiseerd en na de test zorgvuldig verwijderd.*

[3] Hoewel 'elektronisch' hier uit principe tussen haken staat, is in het bestek van deze notitie de gangbare praktijk dat 'testen' vrijwel altijd het geautomatiseerd elektronisch verwerken van gegevens inhoudt. In de wet en in dit document wordt geen onderscheid gemaakt tussen handmatige en geautomatiseerde verwerking.

[4] Voor de volledigheid: de voor persoonsgegevens vereiste zorgvuldigheid kan ook gewenst zijn op (overige) vertrouwelijke bedrijfsinformatie ('company confidential'); daarvoor ontbreekt echter een wettelijke basis, behalve voor de Rijksoverheid (VIR-BI) http://wetten.overheid.nl/BWBR0016435/.

2.2 Persoonsgegevens

De Wbp hanteert voor een *Persoonsgegeven* de volgende definitie: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.

Het begrip persoonsgegeven omvat elke vorm van informatie die, afzonderlijk of in combinatie met andere informatie die binnen dezelfde context van het gebruik gevonden kan worden, kan leiden tot de identificatie van een natuurlijke persoon. In de praktijk kan het gaan om een of meer elementen uit een testbestand (of: testbestanden) die aan elkaar worden gerelateerd in het kader van een test. Een natuurlijk persoon is in het kader van deze notitie een levende persoon waaraan rechten en verplichtingen kunnen worden toegekend.[5]

2.3 Productie en testomgeving

Een testomgeving is in principe nooit tegelijk ook een operationele productieomgeving. In ieder geval wordt in deze richtlijnen gesteld dat beide omgevingen altijd strikt (logisch) van elkaar gescheiden moeten zijn.

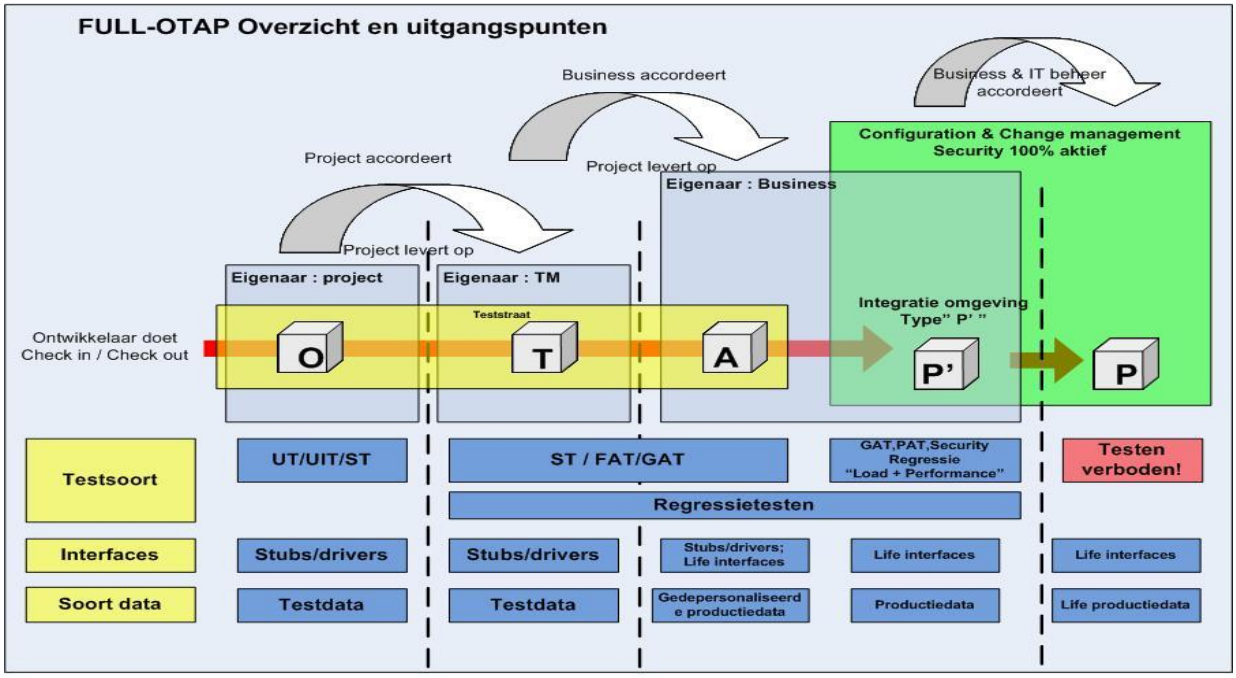

fig.1: niet testen op productie.

3 Uitgangspunten

3.1 Niet testen met persoonsgegevens. Tenzij...

Persoonsgegevens mogen alleen verwerkt worden voor de doeleinden waarvoor ze zijn verkregen (Wbp artikel 9). Dit is het doelbindingsprincipe. Er worden niet méér persoonsgegevens verwerkt dan noodzakelijk voor de doeleinden waarvoor ze zijn verkregen (Wbp artikel 11). Dit is het proportionaliteitsbeginsel. Beide beginselen leiden tot het "need to know principe". In de praktijk: persoonsgegevens zijn uitsluitend toegankelijk voor zover strikt noodzakelijk. Ook in testsituaties.

[5] Een overleden persoon valt niet onder de Wbp. Dat wil niet zeggen dat het gebruik van gevoelige gegevens van overleden personen niet problematisch zou kunnen zijn.

Principieel kan worden gesteld dat het gebruik van tot natuurlijke personen herleidbare informatie niet is verstrekt ten behoeve van het testen van de functionele werking van applicaties.
Los daarvan kleven aan het gebruik van dergelijke gegevens in testen risico's, zeker wanneer de te testen programmatuur modules bevat die contact kunnen maken met printers, e-mail-programma's of serveradressen buiten de eigen organisatie (ketenverwerking).[6]

Het vertrekpunt voor beleid kan daarom zijn dat (kopie)bestanden met tot natuurlijke personen herleidbare informatie nooit als gegevensbestand mogen dienen voor het uitvoeren van testen.
De - technische - oplossing is gelegen in anonimiseren of fingeren van gegevensbestanden.
Een geanonimiseerd of gefingeerd testbestand is in de regel een bestand waarin de bestands-structuur wordt gehandhaafd maar waaruit op geen enkele manier een natuurlijke persoon kan kunnen worden getraceerd.
Er doen zich evenwel situaties voor waarin testen met gefingeerde gegevens om technische redenen geen optie is. Afzien van anonimisering verplicht dan tot strikt na te leven - aanvullende - organisatorische maatregelen.

3.2 Afwegingen

De Wbp legt de beoordeling, of verwerking van persoonsgegevens als onverenigbaar kan worden gezien met de doeleinden waarvoor ze zijn verkregen, bij de 'verantwoordelijke' (art 9 Wbp).
Dit is in de regel de organisatie, die in elk geval het volgende moet toetsen:

- Bestaat er verwantschap tussen het doel waarvoor de gegevens gebruikt gaan worden en het doel waarvoor de gegevens zijn verkregen?
- Wat is de aard van de gegevens?
- Wat zijn de gevolgen van de beoogde verwerking voor de betrokkene?
- Hoe zijn de gegevens verkregen?
- Welke passende maatregelen worden getroffen jegens de betrokkene?

Voor de uitvoering van de wettelijke taken door een uitvoeringsorganisatie is het gebruik van gegevensverwerkende programmatuur een noodzakelijk vereiste geworden. De verantwoordelijke (organisatie) zorgt voor een efficiënte en veilige verwerking van gegevens en heeft daarbij een verantwoordelijkheid voor het zorgvuldig omgaan met privacygevoelige persoonsgegevens van de klanten. Hoewel persoonsgegevens doorgaans niet worden verstrekt ten behoeve van het testen van de functionele werking van applicaties, kan een doelverwantschap niet worden ontkend.

Een betrouwbare programmatuur maakt de wettelijke taakuitvoering mogelijk, waarvoor de gegevens zijn verkregen. Het is daarom alleszins redelijk te redeneren dat over werking van gegevensverwerkende programmatuur zekerheden moeten bestaan vóórdat er persoonsgegevens mee worden verwerkt. De betrouwbaarheid, integriteit en robuustheid van gegevensverwerkende applicaties is immers ook in het belang van de klant.

Van belang is de *aard* van de betreffende gegevens. Hoe gevoeliger het gegeven, des te minder snel mag worden aangenomen dat er sprake is van verenigbaar gebruik indien bij enige verwerking wordt afgeweken van het oorspronkelijk doel. Zijn de gegevens van de betrokkene zélf verkregen en worden er bovendien met het oog op het belang van de betrokkene passende waarborgen geboden, dan is de kans groter dat aan de voorwaarde van verenigbaar gebruik is voldaan.

Voorts is van belang in welke mate de betrokkene de *gevolgen* ondervindt van een doelwijziging. De persoonsgegevens in testsituaties mogen niet worden gebruikt als basis voor mogelijke beslissingen. Het testen van de applicaties heeft geen gevolgen voor de rechtspositie van de betrokkene.

---

[6] Het is voorgekomen dat een overheidsorganisatie vanuit een testsituatie volstrekt ten onrechte duizenden brieven heeft verstuurd naar actuele klanten (persoonlijke communicatie, rdb).

3.3 Technische bezwaren en kosten

Er kunnen twee bezwaren zijn tegen het testen met gefingeerde of geanonimiseerde productiegegevens: het kostenaspect en de non-representativiteit van de test.

3.3.1 Onevenredige kosten

Er kunnen speciale testbestanden met gefingeerde gegevens worden gemaakt en/of bestaande productiegegevens kunnen geanonimiseerd worden. Waar dat mogelijk is en volstaat voor de uit te voeren testen, moet dat worden nagestreefd.
Daarbij mag een kostenafweging worden gemaakt, die ertoe zou kunnen leiden toch hiervan af te zien. De Wbp (art. 13) en vigerende algemene normenkaders laten de deur op een kier voor het gebruik van 'real life data', wanneer effort en kosten niet meer in redelijke verhouding staan tot het doel. De risico's moeten dan wel worden gedempt door aanvullende maatregelen om ongeoorloofde toegang tot de persoonsgegevens te voorkomen. In wezen behelzen deze maat-regelen niets anders dan alle zorgvuldigheid die de organisatie hiervoor toch al moet betrachten, met daarbij ook de nodige aandacht voor de typische kenmerken in geval van uitbesteding:

- Vreemd personeel;
- Transport
- Toegang;
- Bewaartermijn
- Vernietiging(sgarantie);
- Procedurele borging, verantwoording, communicatie.

Het is aan te bevelen bij het organiseren van testen en testsituaties een praktijk van 'verhoogde dijkbewaking' in te stellen, in ieder geval een 'scherpe' dijkbewaking.

Over de diverse aspecten van organisatorische beveiliging is al veel materiaal beschikbaar in vigerende (audit)normensets als de Code voor Informatiebeveiliging, de BIR-TNK en de ISO27xxx. Ook hebben - in ieder geval de grotere - ZBO's binnen de SUWI-keten daarvan uitgebreide eigen bewerkingen/uitwerkingen met richtlijnen, voorbeeldcontracten en protocollen die als ready-mades kunnen fungeren.
Over de prijsafweging is daarentegen geen (openbaar) materiaal. De CBP-richtsnoeren geven aan dat de afweging in relatie tot de risico's gemaakt mag worden en mag leiden tot gecontroleerd gebruik van de productiedata, maar geeft daarvoor geen financiële indicatie of vuistregel.[7]

3.3.2 Verschillende soorten testen en representativiteit

Anonimisering/scrambling is voor testen niet altijd nodig, en als het wel nodig of wenselijk is, dan zijn daar instrumenten voor. Maar soms is anonimisering eigenlijk geen optie.

De testsoorten, waarbij noodzaak en kosten een rol spelen, zijn:

- Applicatietesten (ontwikkelfase): behandelt de applicatie de gegevens integer, voorspelbaar, betrouwbaar en 'secure'?
- Functionaliteit: doet de aangepaste of ontwikkelde software wat de business heeft besteld?
- Connectiviteit: wordt informatie onaangetast verstuurd en ontvangen binnen het eigen IT-landschap en in dataverkeer met applicaties buiten de eigen omgeving?
- Loadtesten: is de applicatie op het te verwachte gebruik berekend? Is de applicatie*keten* op het te verwachte gebruik berekend?

Als we ervan uitgaan dat testen voor het overgrote deel worden uitgevoerd door mensen die vanuit hun functie géén toegang behoren te hebben tot persoonsgegevens van anderen, dan behoort anonimisering van dergelijke gegevens in de testset de aangewezen werkwijze te zijn.

---

[7] Een van de reviewers stelt voor: anonimisering mag hooguit 5% van het totale testbedrag bedragen.

Echter: bij alle genoemde testsoorten, met uitzondering wellicht van de connectiviteitstesten, is het soms niet wenselijk om gefingeerde bestanden te gebruiken, omdat daarmee niet gegarandeerd is dat de werkelijke productiesituatie voldoende betrouwbaar wordt getoetst.

3.3.3 BSN/GBA-check/ketentesten

Veel van de persoonsgegevens in de productiestraten van organisaties zijn of worden gekoppeld aan een BSN-nummer. Met name de bestanden in SUWI-ketens (bijvoorbeeld: de loonaangifte-keten) zijn bekende gevallen. Dit maakt testen dikwijls complex.

Een BSN-nummer is niet willekeurig en moet voldoen aan rekenkundige vereisten. Bovendien zijn valide BSN-nummers uniek gekoppeld aan personen. Dat betekent dat je in de testsituatie de GBA-check uit moet kunnen zetten, omdat anders de persoonsgegevens die bij het al dan niet gefingeerde verzonden BSN-nummer horen, tijdens de test worden teruggeleverd aan de applicatie. Doorgaans zijn de overige persoonsgegevens gescrambled (onherkenbaar gemaakt), zodat het foutmeldingen zal regenen en de test niet representatief kan zijn.

Bij de 'lokale' applicatietesten (integraal of op onderdelen) is dat risico doorgaans goed in te schatten en zal vaak een compacte, vaste testset met gefingeerde gegevens kunnen volstaan om de werking van de applicatie trefzeker te kunnen testen. Logius heeft hiervoor een beperkte set van 'test-BSN-nummers'.
Voor loadtesten kun je een compacte testset vaak eenvoudigweg vermenigvuldigen.

Verschillende leveranciers (w.o. IBM, Oracle) bieden instrumenten aan waarmee de datastructuur ongewijzigd kan blijven terwijl de gegevens op veldniveau acceptabel worden verminkt. De geavanceerde versies kunnen dat desgewenst voor een gedeelte van de velden doen, zodat overige velden ongeschonden getest kunnen worden.

Voor testen in ketenverband volstaat de testset van Logius of anonimiseren doorgaans niet. Dit levert met name bij integrale ketentesten met systemen van andere organisaties een speciaal dilemma op. Daar vormt enerzijds de BSN-problematiek een obstakel voor scrambling, maar kun je anderzijds ook beargumenteren dat een 'ketensituatie', waarbij meerdere organisaties en systemen betrokken zijn, waarschijnlijk nooit met louter organisatorische maatregelen afdoende te beveiligen is. Het is waarschijnlijk om deze reden dat de Suwi Domeingroep Privacy en Beveiliging stelt dat het gebruik van productiedata niet is toegestaan in ketentesten. En daarmee is dan een patstelling bereikt.[8] [9]

Naar mate het stadium van inproductiename nadert, moeten de testen doorgaans 'realistischer' worden. Wanneer de finale testen, vlak vóór en na de desbetreffende release, worden gedaan door het eigen personeel dat ook in het dagelijks werk met de desbetreffende persoonsgegevens werkt, dan is het specifieke testrisico ten opzichte van de productiesituatie feitelijk nihil en kunnen ingrijpende maatregelen achterwege blijven.

3.4 Risicoprofielen van persoonsgegevens

Niet alleen de manier van verwerking, maar ook de aard van de te beschermen gegevens brengen verschillende risicoprofielen met zich mee. Niet alle gegevens zijn in gelijke mate risicovol voor personen of organisaties wanneer zij in onbedoelde handen vallen.

---

[8] Er zijn, in ieder geval binnen de Suwiketen, disputen over de vormgeving van deze brede ketentesten (persoonlijke communicatie, rdb)

[9] Zie par. 3.7 van de publicatie van de Suwi domeingroep Privacy en Beveiliging: *DPB0397f Richtlijn gebruik productiegegevens v1.0.doc, BKWI 2005*. http://www.bkwi.nl/uploads/media/Richtlijn_gebruik_productiegegevens.pdf

Tot februari 2013 werd in dit verband doorgaans verwezen naar een breed geaccepteerd stelsel van risicoklassen en de daaraan verbonden beschermingsmaatregelen van de studie van G.W. van Blarkom en J.J. Borking "*A&V23: Beveiliging van persoonsgegevens*"(Registratiekamer, 2001).

3.4.1 Risicoklasse vs. actuele risico-inschatting

Hoewel A&V23 nooit als norm is gepositioneerd, is het in de loop der jaren wel een de facto standaardbenadering geworden. De A&V23 schreef op basis van een risicoclassificatie (I-II-III) beveiligingsmaatregelen voor. De risicoclassificatie was gebaseerd op de (statische) aard van de verwerkte persoonsgegevens in combinatie met de hoeveelheid verwerkte persoonsgegevens en de complexiteit van de verwerking. Een risicogerichte benadering, waarbij *op basis van analyse van de feitelijke risico's in een gegeven situatie* gerichte beveiligingsmaatregelen worden getroffen, ontbrak.

3.4.2 CBP-Richtsnoeren

Als gevolg van het statische karakter van het classificeringsmodel is A&V23, in ieder geval waar het gaat om het concreet treffen van beveiligingsmaatregelen, in de loop der jaren steeds verder af komen te staan van de beveiligingspraktijk.
Met de inwerkingtreding van de *Richtsnoeren beveiliging van persoonsgegevens* (CBP, feb 2013) heeft het CBP zelf A&V23 daarom vervangen door diezelfde Richtsnoeren.

In de richtsnoeren kiest het CBP nu voor dynamische risicoanalyse: per toepassing/situatie kunnen risico's en daarmee ook de beschermingsmaatregelen verschillen. Deze maatregelen moeten in een verslag van de risicoafweging verantwoord worden op basis van een onderliggend risicoanalyserapport. Zo bieden de Richsnoeren de flexibiliteit om die beveiligingsmaatregelen te treffen die in de gegeven situatie het meest passend zijn naar het oordeel van de gegevenseigenaar.

Toch biedt het concept van risicoklassen nog volop concrete handvatten voor beleid en uitvoering. Het CIP geeft daarom graag de suggestie mee om in ieder geval het idee niet zomaar overboord te zetten, maar te combineren met de nieuwe CBP-Richtsnoeren. Adopteer (en zonodig: adapteer) het risicoklassenstelsel van A&V23 als eigen organisatienorm voor een globale voorsortering met het oog op de verwerking van persoonsgegevens, waarin - bijvoorbeeld - klasse III gegevens al bij voorbaat structureel kunnen worden uitgesloten van ongeanonimiseerd gebruik in testsituaties.

Voer daarna, wanneer nodig, de door de Richtsnoeren voorgeschreven risicoanalyses uit en leg deze vast voordat een testsituatie wordt gerealiseerd.

3.5 Samenvatting

Buiten de productieomgeving wordt als norm géén gebruik gemaakt van persoonsgegevens.
Indien wordt afgeweken van deze norm dan vindt de afweging per afzonderlijke gebeurtenis of situatie plaats, gebaseerd op de noodzaak en het ontbreken van alternatieven.
Iedere afweging wordt altijd vooraf goedgekeurd door de gegevenseigenaar en is gebaseerd op:

- Risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen;
- Kosten van de tenuitvoerlegging.

De benodigde passende maatregelen worden vooraf bepaald; de risico-analyse en de besluit-vorming worden transparant geadministreerd. Gebruik van een stelsel van risicoklassen kan daarbij behulpzaam zijn.

In bijlage 1 vindt u een uitgebreide checklist.

4 Anticiperen

Het is belangrijk om deze (nieuwe?) praktijk in de organisatie goed te verankeren in de bedrijfsprocessen die raken aan de verwerking van persoonsgegevens buiten de productie-omgeving: applicatieontwikkeling en testen in het bijzonder. Dit vereist een toets- en acceptatiekader en de nodige organisatiemaatregelen, en bovenal: het als vanzelfsprekend accepteren van deze praktijk. Het volstaat eenvoudigweg niet meer om alle gegevens en gegevensverwerkingen categorisch als klasse II te bestempelen, met een uitzondering voor gegevens over seksuele geaardheid of medische conditie, die in A&V23 klasse III zouden vallen.

4.1.1 Maturity assessment

Bij de organisatorische borging van maatregelen voor risico-analyse vóóraf hoort ook het vastleggen en transparant maken van besluitvorming - zeker wanneer er bewust voor wordt gekozen af te wijken van de baseline (comply or explain).[10]
Dit past naadloos in de systematiek van het werken met 'Capability Maturity Models' (CMM), die met name de laatste tijd nogal in de belangstelling is gekomen. Het CIP (te weten: de domein-groep Normen) werkt aan een rechtstreekse verbinding tussen normen/normenkader en maturity assessment. Ook zijn er zeker raakvlakken te benoemen met de op handen zijnde nieuwe Europese Privacyverordening.

4.1.2 De Europese privacyverordening

De verordening is nog niet definitief. Maar vrijwel zeker zullen veel richtlijnen met betrekking tot de verwerking van persoonsgegevens strenger worden - dan wel preciezer moeten worden nageleefd, bijvoorbeeld omdat ook de informatieplicht zwaarder wordt.

Verantwoordelijken krijgen meer verplichtingen, waaronder de navolgende, die enige relatie hebben met persoonsgevens in testsituaties. En greep uit de dingen die - althans in de concepten - op stapel staan:

- Strengere regels met betrekking tot het verantwoorden van gegevensverwerking.
- De informatieplicht wordt zwaarder. Verantwoordelijken dienen betrokkenen op een duidelijke, eenvoudig toegankelijke en begrijpelijke wijze te informeren over de verwerking van persoonsgegevens. Nieuw is dat verantwoordelijken betrokkenen moeten informeren over de periode van opslag van de persoonsgegevens.
- Meldplicht datalekken. Datalekken dienen zo spoedig mogelijk, binnen 24 uur na bekend worden, door verantwoordelijken gemeld te worden aan de nationale toezichthouder. Tevens is er een meldplicht jegens betrokkenen.
- Uitdrukkelijke toestemming. Uitgangspunt is dat verantwoordelijken uitdrukkelijke toestemming van betrokkenen dienen te krijgen voor het verzamelen en gebruiken van gegevens. Voor direct mail en telemarketing is een uitzondering gemaakt; hiervoor blijft opt-out gelden. Uitdrukkelijke toestemming is strenger dan de ondubbelzinnige

[10] Een van de reviewers meldt dat in zijn organisatie (systeem)eigenaren bij het bewust afwijken van of niet kunnen voldoen aan een norm een risico-acceptatieformulier (RAF) ondertekenen. Hiermee leggen ze expliciet de verantwoordelijkheid vast voor het te lopen risico, waarop teruggegrepen kan worden bij een incident. Dit zou ook door de gegevenseigenaar onder-tekend kunnen worden bij de goedkeuring voorafgaande aan testen met persoonsgegevens. Zodoende kun je tevens voldoen aan het 'comply or explain' principe van de BIR TNK.

toestemming die nu in de Wbp is opgenomen.[11] Voorts geldt dat de bewijslast bij de verantwoordelijke ligt.

- Databeveiliging. Nieuw is dat, onafhankelijk van contractuele afspraken met verantwoordelijke, ook bewerkers verantwoordelijk zijn voor databeveiliging.

Het vermoeden bestaat dat veel organisaties hier nog wel wat huiswerk aan zullen hebben.

[11] Voor uitdrukkelijke toestemming moet de betrokkene expliciet zijn wil hebben geuit. Dit vereist een actieve houding van betrokkene. Een stilzwijgende of impliciete toestemming is onvoldoende. Voor ondubbelzinnige toestemming geldt dat alle twijfel moet zijn uitgesloten over de vraag of de betrokkene zijn toestemming heeft gegeven en voor welke specifieke verwerkingen toestemming is gegeven. Het verifiëren hiervan hoeft niet noodzakelijkerwijs te leiden tot het vragen van uitdrukkelijke toestemming.

Bijlage 1: Principes voor het gebruik van persoonsgegevens in testbestanden

In aanvulling op paragraaf 3.5 volgt hieronder een uitgebreide lijst van principes voor het gebruik van persoonsgegevens in testbestanden. De principes zijn gerelateerd aan de risicoklasse die bij het UWV aan de persoonsgegevens is toegekend[12]. Een relatie met risicoklassen is optioneel.

	Checklist van te hanteren principes	**RK-I**	**RK-II**	**RK-III**
Algemene verantwoordelijkheden				
	De gegevenseigenaar maakt een afweging voor gebruik van (leesbare/ niet geanonimiseerde) persoonsgegevens voor testdoeleinden op basis van: • De noodzaak en het ontbreken van alternatieven • De kosten van de tenuitvoerlegging; • De aard van de te beschermen gegevens en de risico's die de verwerking met zich meebrengt; De afweging geldt per testsoort en niet voor een gehele testcyclus.	●	●	●
	De gegevenseigenaar documenteert de afweging, indien (leesbare/niet geanonimiseerde) persoonsgegevens buiten productie gebruikt worden.	●	●	●
	De partij of persoon die testen uitvoert met actuele persoonsgegevens uit productie ('tester') kent de normen, waaraan de beveiliging van persoonsgegevens moeten voldoen en heeft de verplichting ze te implementeren. Voor de normen geldt dat de tester minimaal hetzelfde niveau van beveiliging garandeert als de gegeveneigenaar. De bijbehorende verplichtingen zijn contractueel vastgelegd.	●	●	●
	De gegevenseigenaar stelt vast dat de beveiligingsmaatregelen overeenkomen met de eisen betreffende: • De beveiligingsmaatregelen en -procedures voor het beveiligen van de verwerking van persoonsgegevens; • De verantwoordelijkheden, bevoegdheden en taken van de betrokken medewerkers conform "need to know"; • Het toezicht houden op de handhaving en naleving van de maatregelen en procedures.	●	●	●
	De uitvoering van en de controle op de beveiligingsmaatregelen zijn gescheiden, zodat deze niet door dezelfde medewerker worden uitgevoerd. Deze functiescheiding wordt bewaakt.		●	●

[12] Direct afgeleid en sterk gelijkend op de risicoklassen van A&V23.

Baseline beveiliging				
	Bij het gebruik van persoonsgegevens buiten productie c.q. in testsituaties gelden de beveiligingsmaatregelen voor gebruik van persoonsgegevens binnen productie als baseline.	●	●	●
	Indien gebruik gemaakt moet worden van een kopie van de productie-gegevens, dan wordt de set van persoonsgegevens zo beperkt mogelijk te houden; dit geldt ook voor de overige gegevenselementen.	●	●	●
	De gegevensverwerking tijdens het testen is niet van invloed op de (productiegegevens in de) bedrijfsvoering en daarmee ook niet op de betrokkene. (Wbp art 9, lid 2c);	●	●	●
	Test- en productieomgeving zijn logisch gescheiden en testgegevens mogen nooit in de productieomgeving komen. Deze maatregelen zijn vastgelegd en kunnen worden aangetoond.	●	●	●
	De toegang tot de gegevens is op basis van "need to know" (Wbp art 9, lid 4)	●	●	●
Personeel en organisatie				
	Personen die toegang krijgen tot testgegevens met productiedata hebben een geheimhoudingsverklaring getekend. Eigen personeel dat test met een kopie van de productiegegevens wordt erop gewezen dat de geheimhoudingsplicht ook geldt voor de testomgeving.	●	●	●
	Medewerkers en derden die te maken krijgen met persoonsgegevens uit de categorie III[13] moeten een verklaring omtrent het gedrag overleggen. Indien verwerking door derden plaatsvindt, maakt een betrouwbaarheids- of veiligheidsonderzoek deel uit van de selectie van de organisatie.			●
Toegang tot persoonsgegevens				
	Het verlenen van toegang is controleerbaar en het aantal personen dat toegang heeft wordt tot een minimum beperkt.	●	●	●
	De tijd dat een tester toegang heeft tot de testomgeving is gelimiteerd tot de duur van de test.		●	●
	Het gebruik van persoonsgegevens wordt door of onder toezicht van de gegevenseigenaar uitgevoerd.			●
	De gedistribueerde kopieën zijn traceerbaar door het voeren van een administratie van de distributie.			●
	Alle gegevensdragers met persoonsgegevens van deze risicoklasse zijn voorzien van een markering waaruit de risicoklasse blijkt.			●

[13] Cf. A&V23 of vergelijkbare gevoeligheid. Deze klasse kan ook van toepassing worden verklaard op vertrouwelijke bedrijfsinformatie ('company confidential'). De Rijksoverheid kent een aanvullende set van maatregelen: het *Voorschrift Informatiebeveiliging - Bijzondere Informatie* (VIR-BI). In dit voorschrift wordt voor 4 categorieën van informatie extra eisen gesteld: Departementaal Vertrouwelijk, Staatsgeheim Confidentieel, Staatsgeheim Geheim, Staatsgeheim Zeer geheim.

Werkplek(-omgeving)				
	Indien verwerking fysiek buiten de eigen organisatie plaatsvindt, gelden hier ook de eisen aan de locatie en de werkplek(-omgeving), zoals die aan de eigen organisatie worden gesteld.	●	●	●
	Bij onderhoud aan of beheer van apparatuur door derden moet de vertrouwelijke omgang met persoonsgegevens in een schriftelijke overeenkomst zijn vastgelegd.		●	●
Netwerken en externe verbindingen				
	Bij datatransport(fysiek of elektronisch) wordt voorkomen dat de (persoons)gegevens kunnen worden gelezen door onbevoegden, over het algemeen minimaal door toepassing van encryptie.	●	●	●
	Toegang tot en vanuit publiek toegankelijke netwerken zoals Internet vanuit of naar de testlocatie vindt gecontroleerd plaats.	●	●	●
	De zend- en ontvangstpunten bij externe datacommunicatie verzekeren zich van elkaars juiste identiteit (zoals bijvoorbeeld door middel van terugbelsystemen, terminal identificatie, verificatie van digitale certificaten).		●	●
	Transport van bestanden of gegevens naar buiten de organisatie of het domein van de gegevenseigenaar is alleen toegestaan nadat de beveiligingsmaatregelen zijn genomen, gedocumenteerd en aangetoond.			●
Bewaren van persoonsgegevens				
	De gegevensdragers met persoonsgegevens moeten zo worden bewaard en behandeld dat alleen bevoegde personen er toegang toe hebben.	●	●	●
	Opslag van testgegevens valt onder de richtlijnen voor bewaartermijnen zoals die gelden voor productiegegevens, met dien verstande dat voor testgegevens de Archiefwet niet van toepassing is en dat de algemene stelregel is: niet langer bewaren dan strikt noodzakelijk.	●	●	●
	Opgeslagen gegevensdragers zijn voorzien van een classificatieaanduiding		●	●
	De gegevensdragers met persoonsgegevens worden in een afgesloten ruimte bewaard. Deze ruimte of de bebouwing daaromheen is voorzien van afdoende maatregelen voor inbraakpreventie en inbraakdetectie.		●	●
	De gegevensdragers worden in een inbraakwerende ruimte (kluis) bewaard. De persoonsgegevens zijn tevens afdoende versleuteld.			●
Vernietiging van persoonsgegevens				
	Testgegevens die actuele persoonsgegevens bevatten worden (aantoonbaar) vernietigd of integraal teruggeleverd na afloop van de test. Hiervan wordt een administratie gevoerd waarin is vermeld welke functionaris, op welk tijdstip, de gegevens heeft vernietigd en wie daartoe opdracht heeft gegeven.	●	●	●

Bijlage 2: Wbp art. 1, 8, 9 en 13

Artikel 1
In deze wet en de daarop berustende bepalingen wordt verstaan onder:

a. persoonsgegeven: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon;
b. verwerking van persoonsgegevens: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens;
c. bestand: elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen;
d. verantwoordelijke: de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of te zamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt;
e. bewerker: degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen;
f. betrokkene: degene op wie een persoonsgegeven betrekking heeft;
g. derde: ieder, niet zijnde de betrokkene, de verantwoordelijke, de bewerker, of enig persoon die onder rechtstreeks gezag van de verantwoordelijke of de bewerker gemachtigd is om persoonsgegevens te verwerken;
h. ontvanger: degene aan wie de persoonsgegevens worden verstrekt;
i. toestemming van de betrokkene: elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt;

(…)

n. verstrekken van persoonsgegevens: het bekend maken of ter beschikking stellen van persoonsgegevens;
o. verzamelen van persoonsgegevens: het verkrijgen van persoonsgegevens.

Artikel 8
Persoonsgegevens mogen slechts worden verwerkt indien:

a. de betrokkene voor de verwerking zijn ondubbelzinnige toestemming heeft verleend;
b. de gegevensverwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst;
c. de gegevensverwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is;
d. de gegevensverwerking noodzakelijk is ter vrijwaring van een vitaal belang van de betrokkene;
e. de gegevensverwerking noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt, of
f. de gegevensverwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert.

Artikel 9

1. Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.
2. Bij de beoordeling of een verwerking onverenigbaar is als bedoeld in het eerste lid, houdt de verantwoordelijke in elk geval rekening met:
   a. de verwantschap tussen het doel van de beoogde verwerking en het doel waarvoor de gegevens zijn verkregen;
   b. de aard van de betreffende gegevens;
   c. de gevolgen van de beoogde verwerking voor de betrokkene;
   d. de wijze waarop de gegevens zijn verkregen en
   e. de mate waarin jegens de betrokkene wordt voorzien in passende waarborgen.
3. Verdere verwerking van de gegevens voor historische, statistische of wetenschappelijke doeleinden, wordt niet als onverenigbaar beschouwd, indien de verantwoordelijke de nodige voorzieningen heeft getroffen ten einde te verzekeren dat de verdere verwerking uitsluitend geschiedt ten behoeve van deze specifieke doeleinden.
4. De verwerking van persoonsgegevens blijft achterwege voor zover een geheimhoudingsplicht uit hoofde van ambt, beroep of wettelijk voorschrift daaraan in de weg staat.

Artikel 13

De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

Referentiedocumentatie

Versie	Datum	Titel	Auteur(s)
def	6 juli 2000	Wet bescherming persoonsgegevens http://wetten.overheid.nl/BWBR0011468/	
	april 2001	Beveiliging van persoonsgegevens Achtergrondstudies en Verkenningen 23	G.W. van Blarkom drs. J.J. Borking
1.0	4-7-2006	UWV: Richtlijn Omgang persoonsgegevens binnen testsituaties	T.Yildirim
3.0	25-8-2011	UWV: Tactisch Beleid Beveiliging & Privacy.	
1.0	19-7-2005	UWV: Classificatiemodel	
1.0	13 maart 2006	UWV: Richtlijnen OTAP omgevingen	Kelvin Rorive/Frank Jan Bijl/Marcel Koers/Fred Pel
1.0	20-12-2005	Richtlijn gebruik productiegegevens (DPB) http://www.bkwi.nl/uploads/media/Richtlijn gebruik productiegegevens.pdf	M. van der Werff, B. de Wit, BKWI, vastgesteld door DPB
	23-6-2011	Verantwoordingsrichtlijn GeVS aangaande de Gezamenlijke elektronische Voorzieningen Suwi: Normenkader GeVS aangaande de GeVS	Jan Breeman/BKWI, DPB
	25-1-2012	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protec-tion Regulation), Brussels, COM(2012) 11 final.	
1.9	18-3-2013	UWV: Persoonsgegevens buiten de productieomgeving	Marcel Koers
def	februari 2013	CBP-Richtsnoeren Beveiliging van persoonsgegevens	CBP
def CIP	3 juni 2013	De Europese Privacy Verordening: strengere privacyregels op komst: http://juristenweblog.nl/artikelen.asp?aid=212	
def CIP	3 juni 2013	http://www.gertkoolwijk.nl/de-baseline-informatiebeveiliging-rijksdienst-bir	
def CIP	3 juni 2013	Voorschrift Informatiebeveiliging - Bijzondere Informatie (VIR-BI): http://wetten.overheid.nl/BWBR0016435/	

Lijst van afkortingen

A&V23	Achtergrondstudies en Verkenningen 23
BIR-TNK	Baseline Informatiebeveiliging Rijksdienst (en Tactisch Normen Kader)
BKWI	Bureau Keteninformatisering Werk en Inkomen
BSN	Burger Service Nummer
CBP	College Bescherming Persoonsgegevens
CMM	Capability Maturity Model (-systematiek)
DPB	Domeingroep Privacy en Beveiliging (in Suwi-verband)
GBA	Gemeentelijke Basis Administratie (voor persoonsgegevens)
GeVS	Gezamenlijke elektronische Voorziening Suwi
ISO	Internationale Organisatie voor Standaardisatie
OTAP	Ontwikkeling Test Acceptatie en Productie
SUWI	Wet structuur uitvoeringsorganisatie werk en inkomen
VIR-BI	Voorschrift Informatiebeveiliging - Bijzondere Informatie (VIR-BI)
Wbp	Wet bescherming persoonsgegevens
ZBO	Zelfstandig bestuursorgaan

Reviewers

Aan deze review van de UWV concept notitie " UWV: Persoonsgegevens buiten de productieomgeving" hebben meegewerkt en bijgedragen:

Wietze Geertsma (ADR/FIN)
Marlies van Eck (Belastingdienst Toeslagen)
Rob Kuppens (CAK)
Gustav van den Berg (CJIB)
Chris Eyzenga (CJIB)
Anne Marie van Rooij (CVZ)
Ad van Etten (DUO)
Appie Kamstra (OM Noord Ned)
Turabi Yildirim (RWS)
Peter de Witte (SVB)
Bas Veul (UWV)
Marleen Hulshof (UWV)
Joseline van Tessel (UWV)
Ruud de Bruijn (UWV/CIP)

Jan Breeman (BKWI): draagt *Richtlijn gebruik productiegegevens versie 1.0 - 20 december 2005* aan als te gebruiken bron (DPB0397f Richtlijn productiegegevens v1.0.doc, BKWI 2005).
Deze BKWI-publicatie vertoont inhoudelijk grote verwantschap met het hier gepresenteerde CIP-document.

Ruud de Bruijn tekent voor verwerking van de commentaren en de omwerking naar dit CIP-document, met dank aan Peter Ruyter (UWV) voor kritisch meelezen en Joseline van Tessel voor de juridische punten op de i.

Oorspronkelijke documentnaam Wordversie: [Testen met persoonsgegevens CIP DEF4.doc]

UWV, Amsterdam, 3 juni 2013