IB&P Richtlijnen OTAP

De vierdeling voorbij

Inhoud

1 Aanleiding IB&P-richtlijnen OTAP

Sinds 2016 is de AVG ook van kracht en wordt privacy by design by default voorgestaan bij vernieuwing en aanpassing van processen en systemen. De bedoeling hiervan is om al in de ontwerpfase privacybescherming van de betrokkene mee te nemen ('by design'), en tevens standaard de meest privacybeschermende instellingen toe te passen ('by default'). Deze eis is een aanvulling op de Wbp en dus nieuw.

De wettelijke tekst wordt door de Autoriteit Persoonsgegevens (AP) als volgt uitgelegd:

- "Privacy by design houdt in dat u als organisatie al **tijdens de ontwikkeling** van producten en diensten (zoals informatiesystemen) ten eerste aandacht besteedt aan **privacyverhogende maatregelen**, ook wel privacy enhancing technologies (PET) genoemd[1]. Ten tweede houdt u rekening met **dataminimalisatie**: u verwerkt zo min mogelijk persoonsgegevens, dat wil zeggen alleen de gegevens die noodzakelijk zijn voor het doel van de verwerking.
- Privacy by default houdt in dat u **technische en organisatorische maatregelen** moet nemen om ervoor te zorgen dat u, als **standaard**, alléén persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat u wilt bereiken.

De uitgangspunten van privacy by design by default hebben beperkt invloed op het bestaande OTAP-beleid uit 2016. In het bestaande beleid zijn de gehanteerde IV principes al uitgewerkt op basis van geclassificeerde dataverwerking.

1.1 Wijzigingen n.a.v. herziening OTAP procedure

Dit herziene beleid heeft geleid tot genuanceerde wijzigingen van een aantal IB&P-richtlijnen OTAP, waarin nadruk wordt gelegd op het doorvoeren van bestaande maatregelen waarbij deze expliciet moeten worden toegepast in plaats van wenselijk wordt verlangd. Indien maatregelen niet mogelijk zijn zal expliciet een motivatie ("explain") voor een afwijking noodzakelijk zijn.
Feitelijk betekent deze wijziging:

- Maatregelen dienen getroffen te zijn om productiegegevens in acceptatieomgevingen te gebruiken of in geval van noodzaak in een testomgeving. Mogelijkheden zijn anonimisering en/of pseudonimisering en/of dataminimalisatie en/of maskeren van gegevens.
- Maatregelen dienen getroffen te zijn om toegang tot de applicatie/gegevens te beperken bij gebruik van productiedata met persoonsgegevens in de acceptatieomgeving. Daarnaast behoren er maatregelen te zijn om handelingen te loggen en het verwijderen/vernietigen / onherkenbaar maken van gebruikte gegevens na een test.

Een wijziging in de richtlijnen betreft ook het hanteren van het begrip anonimiseren. Met de AVG is er één type van anonimiseren. De drie soorten anonimisering zoals in bestaande beleid werd gehanteerd is gewijzigd naar gebruik van pseudonimisering en anonimisering, waarbij rekening gehouden dient te worden met het uitgangspunt passende maatregelen te treffen die een passend beveiligingsniveau garanderen.

[1] https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/technologie/witboek_pet.pdf

De verwijzing naar de Wbp risico classificatie van data is verwijderd, omdat de AVG geen classificaties hanteert. Nu wordt verwezen naar de UWV BIV classificatie van BZ[2].
Tenslotte is een sjabloon als bijlage toegevoegd ten behoeve van de bepaling/voorwaarden om productiedata met persoonsgegevens te kunnen gebruiken in een acceptatieomgeving. Het principe van privacy by design en by default is hierbij het uitgangspunt.

1.2 Toelichting OTAP

OTAP staat voor Ontwikkel, Test, Acceptatie en Productie. De bedoeling is dat bij elke wijziging of vernieuwing van software deze stappen opeenvolgend worden doorlopen. Het idee is dat software in elke stap zorgvuldig ontwikkeld en/of getest wordt, voordat het gecontroleerd wordt gepromoveerd naar een volgende fase in het voortbrengingstraject.

Het OTAP-proces is gericht op het - op een gedocumenteerde, gecontroleerde en veilige manier - in productie nemen van applicaties, waarbij de stabiliteit en integriteit van de (productie) gegevens gegarandeerd moet zijn en blijven [bron: OTAP-analyse rapport].

UWV is voor haar bedrijfsvoering in belangrijke mate afhankelijk van haar informatievoorziening. Het belang van onze informatievoorziening als *productiemiddel* én als *bewijsmiddel* moet niet onderschat worden.
Een belangrijk deel van onze klantcommunicatie vindt via de internetportalen plaats. Onze medewerkers zijn afhankelijk van onze primaire systemen. Uitval van de informatievoorziening leidt tot productieverlies, imagoschade, herstelwerkzaamheden en de daarbij komende extra kosten. De *beschikbaarheid* van onze informatievoorziening is daarmee van eminent belang.
Onze primaire systemen hebben daarnaast een essentiële rol als *bewijsmiddel.* Onze systemen bevatten de primaire registratie van persoonsgegevens, rechten, hoogte en duur. De controles in en op onze systemen bepalen dus mede de bewijskracht van onze beschikkingen. Of ons digitale bewijs standhoudt voor de rechtbank, hangt af van de *integriteit* van onze informatievoorziening.

Het is dus essentieel dat de (primaire) systemen van UWV beschikbaar, integer en beschermd tegen ongeautoriseerde waarneming zijn. Om aan deze (BIV) eisen te voldoen, moet onze software zorgvuldig ontwikkeld en getest worden. UWV gebruikt een OTAP-ontwikkelstraat om het zorgvuldig ontwikkelen van software af te dwingen.
Uitgangspunt voor de IB&P-richtlijnen is dat deze ervoor zorgen dat:

- Werken in alle omgevingen (be)veilig(d) gebeurt
- UWV beschikt over goede basisafspraken voor:
    - nieuwe ontwikkelingen (zoals ketentesten en Agile)
    - tactische processen (en afspraken) met de leveranciers
- UWV beschikt over een vertrekpunt voor
    - het oplossen van de bestaande ongewenste situaties
    - het ver(der)gaand optimaliseren van de voortbrengingsprocessen (VBP), inclusief de daarbij behorende beheer- en controleprocessen

De IB&P-maatregelen mogen er echter niet toe leiden dat de kwaliteit van de (UWV-)dienstverlening en de kwaliteit van de ontwikkelde software geschaad worden.

[2] Document: UWV BZ BIV classificatie v 1.05

1.3 Herziening IB&P-richtlijnen OTAP - procesmatig

De IB&P-richtlijnen OTAP kennen de onderstaande versiehistorie.

Versie		Datum	Distributie
-	Diverse draft versies		
0.6	Eerste concept	5 april 2016	IB&P-coördinatoren, individuele contactpersonen binnen LeveranciersManagement, Test Service Centrum en CIO-office
0.8	Herziene versie n.a.v. reviewcommentaren op versie 0.6	4 oktober 2016	Business Security Officers, IB&P-coördinatoren Individuele contactpersonen binnen service delivery, functioneel beheer, Test Service Centrum en UCRA
0.86	Concept voor afstemming in de AB op basis van 0.8	24 oktober 2016	Architectuur Board
0.9	Finaal concept na verwerking reviewcommentaren	9 november 2016	Architectuur Board, afschrift aan indieners reviewcommentaar
0.95	Finaal concept na verwerking reviewcommentaren TSC	22 novem-ber 2016	Architectuur Board, afschrift aan indieners reviewcommentaar
1.00	Vastgesteld in AB 24 november 2016	24 nov. 2016	Publicatie via internet en verstrekking aan direct betrokken
1.01	Herziene conceptversie i.v.m. invoering AVG	1 mei 2018	CISO-office intern
1.02	Conceptversie na interne review	7 mei 2018	Juridische zaken, C-ICT architect, Test Service Centrum, AVG/TDA regieteamleden
1.03	Conceptversie na review belanghebbenden	24 mei 2018	AVG/TDA regiegroep, Architectuurboard, Tactische coalitie
1.04	Conceptversie na review TDA regiegroep	15 juni 2018	AVG/TDA regiegroep, Architectuurboard, Tactische coalitie
1.05	Verwijzing naar document BZ BIV classificatie aangepast i.v.m. nieuwe versie	18 juli 2018	IV team
1.06	Versie na goedkeuring IV team	24 juli 2018	Concept verwijderd
1.1	Bijlage G02 en sjabloon tekstueel verbeterd	27 juli 2018	Publicatie via intranet en verstrekking aan relevante partijen

Met deze versie zijn de wijzigingen n.a.v. de AVG – eisen doorgevoerd.

1.4 Doel

De IB&P richtlijnen OTAP, hierna *richtlijnen* genoemd, kennen drie hoofddoelen:

1. Het bieden van duidelijke uitgangspunten m.b.t. informatiebeveiliging en privacy. Het maakt expliciet wat –ook met het oog op de striktere wetgeving- in de OTAP is toegestaan;
2. Het legt de basis voor (be)veilig(d) werken. Het geeft aan welke beveiligingseisen gesteld worden;
3. Duidelijke spelregels neerleggen voor datatransporten binnen de OTAP domeinen, zowel intern als extern

De richtinggevende uitspraken zijn gebaseerd op de IV-principes en het beleid. In de uitspraken is kort toegelicht wat vanuit IB&P-oogpunt is toegestaan op basis van de door het IV-Team vastgestelde principes en beleid.

De richtlijnen gaan uit van combinaties van softwareontwikkeling en het reproduceerbaar kunnen opbouwen van configuraties en representatieve test-situaties. De richtlijnen bieden de kaders om software goed en veilig te ontwikkelen én te gebruiken. De richtlijnen gaan daartoe uit van *Regimes*. Een regime is een geheel van techniek, processen, mensen en maatregelen. UWV kent idealiter drie regimes: Productie, Ontwikkel en Testen. Elk regime is van toepassing op één of meer (deel)omgevingen. Zo

vallen zowel P- als A-omgevingen onder het P-regime, maar mogen ontwikkelwerkzaamheden alleen op een O-omgeving, onder het O-regime worden uitgevoerd.

Regimes beschrijven kort gezegd:
- De werkzaamheden die op een omgeving mogen worden uitgevoerd;
- De spelregels voor a) zowel functionarissen die op die omgeving werken als b) de Ontwikkel- en Hulpprogrammatuur (O&H-programmatuur) die in een omgeving is toegepast;
- De gegevens die in een omgeving en/of regime veilig kunnen worden verwerkt.

Het IB&P-beleid OTAP stelt eisen aan de drie regimes voor wat betreft representativiteit, *rechten en toegang, isolatie en beheersing.* Per regime is beschreven *waartoe* een omgeving dient en wat voor die hoofdtaak nodig is.

1.5 Reikwijdte

De reikwijdte omvat de OTAP omgevingen ter voortbrenging van applicatie-software, ten aanzien van de informatievoorziening van het UWV maar ook die van ketenpartners, voor zover daar werkzaamheden plaatsvinden waar gegevens van UWV worden gebruikt en met name waarbij persoonsgegevens in zijn betrokken.

1.6 samenhang kaders, beleid en richtlijnen

Wet- en regelgeving (Avg).
UWV richtinggevende IV principes en beleid
UWV Privacy beleid, GEB.
Relevante IBP Standaarden, beleid en richtlijnen zoals UWV ICT Richtlijn Test Data Anonimisering, beleidskader Privacy by design en by default, NONGA richtlijnen, richtlijnen UCRA, Handreiking Red envelop controlled access procedure, ontheffing CSD.

1.7 Doelgroep

Deze handreiking is in de eerste plaats bedoeld voor iedereen die op de een of andere wijze betrokken is bij het ontwerpen of de ontwikkeling van software, informatiesystemen en processen.

Maar ook leidinggevenden die betrokken zijn bij de bedrijfsprocessen waarin persoonsgegevens worden verwerkt zijn belangrijk als doelgroep.
Daarnaast is het bedoeld voor andere belanghebbende buiten het UWV, zoals het ministerie van Sociale Zaken en Werkgelegenheid (SZW), de Autoriteit Persoonsgegevens (AP), leveranciers en ketenpartners waarmee een goede aansluiting moet zijn, werkgevers en burgers.

De uitgewerkte richtlijnen zijn van belang voor de B&P-coördinatoren en/of BSO (hierna securityfunctie van de divisie genoemd) en de centrale securiftyfunctie.

1.8 Leeswijzer

In hoofdstuk 2 wordt de OTAP richtlijn en de uitgangspunten voor de uitspraken op IB&P-gebied toegelicht.
In hoofdstuk 3 zijn de uitspraken uit het UWV strategie en beleid vertaald naar IB&P-richtlijnen OTAP

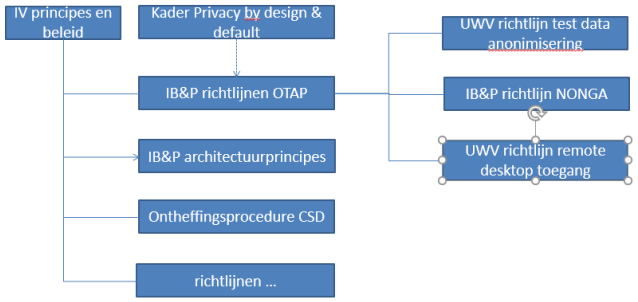
In hoofdstuk 4 is per regime (OTAP) kort benoemd welke richtlijnen van toepassing zijn ten aanzien van toegestane 'niet functionele werkzaamheden' (zoals ontwikkelen, testen, beheer etc) om onze IV-systemen te laten functioneren.
De bijlage bevat de reeds uitgewerkte richtlijnen van de niet-functionele werkzaamheden.

2 Toelichting IB&P-richtlijnen OTAP

Hieronder zijn de IB&P-richtlijnen OTAP en de plaats in de beleidsboom toegelicht.

Figuur 1 – Plaats IB&P-richtlijnen in beleidsboom UWV

Zowel de bestaande richtlijnen Nonga, UCRA, Testdata anonimisering als de IB&P-richtlijnen OTAP (dit document) zijn gebaseerd op de IV-principes en het IV-beleid. Alle richtlijnen bevatten een combinatie van uitspraken over het wat en het hoe (uitgewerkte richtlijnen).
De richtlijnen behandelen de "wat"- en de "hoe"-vraag gescheiden. De 'wat'-vraag wordt behandeld in de eerste drie hoofdstukken. De 'hoe' -vraag wordt beantwoord in hoofdstuk 4 en de bijlage.



Invoeren en operationaliseren uitgewerkte richtlijnen

De richtinggevende uitspraken in hoofdstuk 3 beschrijven de ambitie van UWV en de eisen waaraan UWV zo spoedig mogelijk moet voldoen. Om aan deze eisen te voldoen, behoort het "hoe" voldoende te zijn uitgewerkt. De CISO stelt richtinggevende uitspraken op en werkt deze met de organisatie verder uit. Pas als een uitgewerkte richtlijn beschikbaar is, kan de organisatie een impactanalyse doen en ook de uitgewerkte richtlijnen vaststellen.

Wat valt wel/niet onder de IB&P-richtlijnen OTAP

De IB&P-richtlijnen OTAP richten zich op de niet-functionele werkzaamheden (NFW). Dit zijn activiteiten zoals operationeel beheer, probleemoplossing of ondersteuning bij software releases. Dit document doet geen (nadere) uitspraken over functionele handelingen, inclusief functionele testen zoals GAT of het verifiëren van systeeminstellingen.

De IB&P-richtlijnen OTAP zijn gebaseerd op de IV-principes zoals in 2016 geldend en de AVG uitgangspunten. De IB&P-richtlijnen OTAP doen uitspraken over:

1. Hoe om te gaan met NFW (niet-functionele werkzaamheden);
2. Hoe in NFW de vertrouwelijkheid en integriteit van de (primaire) systemen, de daarin verwerkte gegevens (dan wel eventuele testdata of kritieke data) beschermd worden.

Dit document bevat uitspraken op twee niveau's:

A. Richtinggevende uitspraken, gebaseerd op de IV-principes en het beleid. In de uitspraken is kort toegelicht wat vanuit IB&P-oogpunt is toegestaan op basis van de door het IV-Team vastgestelde principes en beleid;
B. Een concrete invulling in uitgewerkte richtlijnen. Een beknopte beschrijving van de werkzaamheden die toegestaan zijn en hoe de organisatie invulling kan geven aan de richtinggevende uitspraken.

De richtinggevende uitspraken komen voort uit de richtinggevende IV-principes en beleid. Deze zijn afgestemd met de AB en worden via het architectuurproces onderhouden. De huidige (en toekomstige) richtinggevende uitspraken zijn in het AB vastgesteld.

Het aanpassen en/of aanvullen van de uitgewerkte IB&P-richtlijnen vindt in samenwerking met de securityfunctie van de divisie plaats, waarna deze in de tactische coalitie worden geformaliseerd.

De IB&P-richtlijnen OTAP kennen twee beperkingen. Allereerst doen de richtlijnen geen uitspraak m.b.t. de stabiliteit van de primaire systemen. Ten tweede moeten voor grootschalige verwerking van vertrouwelijkheidsklasse 2 gegevens of de verwerking van vertrouwelijkheidsklasse 3 gegevens aanvullende maatregelen overwogen worden. De securityfunctie van de betrokken divisie kan hiervoor contact zoeken met het CISO-office.

2.1 Rationale IB&P-richtlijnen OTAP afkomstig uit IV principes

Het uitgangspunt voor de uitspraken op IB&P-gebied is het eerste IV-principe.

Toelichting	De stabiliteit en continuïteit, inclusief informatiebeveiliging van onze ICT hebben de komende jaren de hoogste prioriteit. UWV is in relatie tot zijn informatiebeveiliging risicomijdend en gericht op het actief voorkomen van *fouten* in, en *inbreuk* op haar IV componenten. Zo wordt proactief voorkomen dat problemen ontstaan, en reactief *tussentijds gecontroleerd* door logging en interpretaties geanalyseerd. UWV stelt eisen aan de ontwikkeling van applicaties, infrastructuur en ketenregie.

De consequentie van bovenstaand principe (PRINCIPE P1, IV-PRINCIPES EN BELEID) zijn:

- Software en configuraties zijn getest voordat ze in productie worden genomen (hoe het feitelijke testen wordt ingevuld, valt buiten deze richtlijn);
- Voor release en onderhoudswerkzaamheden zijn ruime, maar gecontroleerde bevoegdheden en O&H-programmatuur beschikbaar;
- Waar het bedrijfskritische en/of privacygevoelige informatie betreft, wordt ongeautoriseerde waarneming tegengegaan;
- Gewenste beïnvloeding van gegevens of applicaties is toegestaan, mits de toegang een bedrijfsbelang dient en gecontroleerd plaatsvindt.

De consequenties van Principe 1 leiden tot drie hoofdeisen. Dit zijn a) Isolatie, b) Data- en softwarekwaliteit en c) Privacy en risicobeheersing. Deze hoofdeisen zijn in hoofdstuk 3 en verder uitgewerkt tot richtlijnen. Beargumenteerde afwijkingen (excepties) van de richtlijnen zijn vanuit IB&P optiek toegestaan, mits eventuele beveiligingsrisico's bekend en beheerst zijn. Deze uitspraak gaat uit van het 'comply or explain'-beginsel, maar gaan tegelijkertijd ook verder. Indien een afwijking tot risico's

leidt, moeten de risico's gemanaged zijn en voorzien zijn van een oplosplan. De centrale beveiligingsfunctie toetst de afdoening van de risico's en het oplosplan.

Excepties zijn in riskletters gedocumenteerd en bekend bij de centrale beveiligingsfunctie van UWV. De verantwoordelijkheid voor de riskletteradministratie is getrapt:

- Alle leveranciers zijn verantwoordelijk voor de volledigheid, correctheid en actualiteit van hun riskletter administratie;
- Leveranciers leveren het USOC een afslag van hun riskletteradministratie.

Om ervoor te zorgen dat excepties worden opgelost en risico's worden teruggedrongen, overleggen ICT (USOC/CISO) en de securityfunctie van de divisie over de riskletter administratie. Doel van het overleg is het oplossen van de exceptie en te komen tot een beheerste en veilige omgeving. Daar waar nodig en relevant zijn in de uitgewerkte richtlijnen concrete afspraken gemaakt.

Rationale
UWV wil dat productionele software goed getest is. Dit betekent dat tegelijkertijd:

- nieuwe (of aangepaste) software of configuraties vooraf goed getest moeten worden. Om die reden hanteren we een scheiding tussen de omgevingen waarin software wordt getest en de feitelijke productieomgeving;
- het testproces geen onnodige belemmeringen mag ondervinden. Dergelijke beperkingen doen immers afbreuk aan de kwaliteit van testen en ondergraven het doel van principe 1.

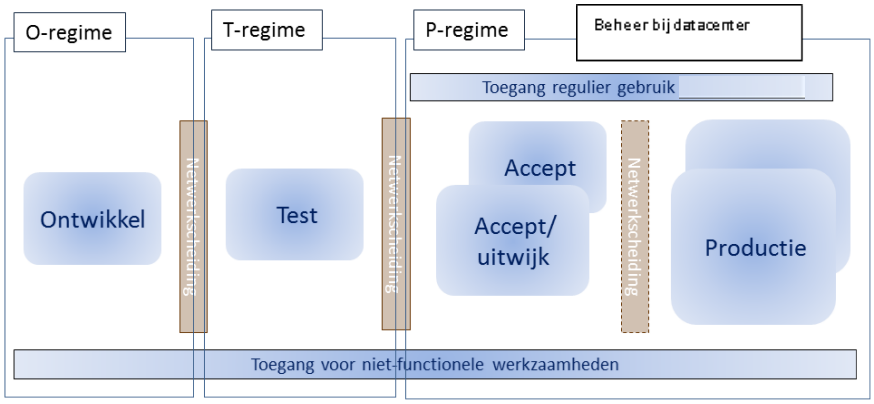
De IB&P Richtlijnen OTAP zorgen voor een gezonde balans tussen veiligheid en werkbaarheid.
De bepaling over koppelingen tussen omgevingen staat gedeeld gebruik van resources onder voorwaarden toe. Dit voorkomt een kostbare doublure van systemen die slechts beperkt gebruikt worden. Interpretaties en logging vereisen dat diverse materiedeskundigen *gecontroleerd* toegang moeten hebben tot instellingen en data.
Hygiëne-eisen zoals één standaardapplicatie en één versie gelden uiteraard ook voor O&H-programmatuur. Deze richtlijn is uitdrukkelijk een nadere invulling van het IT-Beleid en Strategie.

2.2 Opbouw IB&P-richtlijnen OTAP

De IB&P-richtlijnen OTAP zijn in twee stappen opgebouwd.
In deel I zijn de IB&P-spelregels voor de OTAP afgeleid van de leidende IV-principes. De voor IB&P relevante IV-principes zijn uitgewerkt naar IB&P-implicaties in hoofdstuk 3. De IB&P-richtlijnen hebben daarmee hun basis in de richtinggevende IV-principes.
De IB&P-implicaties vormen op hun beurt de basis voor uitgewerkte IB&P-richtlijnen. De uitwerking vindt in samenwerking met de ontvangende organisatie plaats. De uitgewerkte richtlijnen zijn opgenomen in hoofdstukken 4 en 5.

2.2.1 Verschil regime en omgeving

Het OTAP-beleid gaat uit van omgevingen en regimes. De omgevingen zijn de feitelijke infrastructuur waarin bijvoorbeeld ontwikkelaars, testers of eindgebruikers hun werk doen. Dit kan de operationele productieomgeving bij onze provider zijn, maar ook (eventueel elders gesourcede) ontwikkelomgevingen. De spelregels voor de omgevingen zijn in andere documenten uitgewerkt, zoals de IV-strategie, het OTAP-analyserapport en diverse richtlijnen.



In de IB&P-richtlijnen OTAP zijn de regimes verder uitgewerkt.
Een regime is het geheel van spelregels voor één omgeving, denk hierbij aan:

- Verantwoordelijkheden
- Risicoafweging
- Toegestane standaard werkzaamheden
- Beheersingsmaatregelen en controle
- Evaluatie en toezicht

2.2.2 Opbouw regime

Een regime heeft dezelfde opbouw:

1. Doel van het regime;
2. Toegestane werkzaamheden en de daarbij behorende functionarissen;
3. Hoe met risico's en toezicht moet worden omgegaan.

2.3 Begrippen en definities

De IB&P-richtlijnen OTAP maken gebruik van de onderstaande definities.

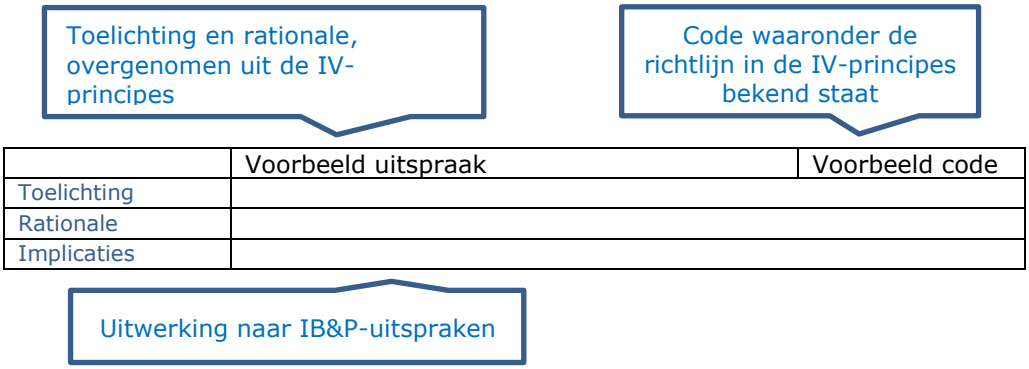
TERM	OMSCHRIJVING
AB	AB staat voor de architectuur board.
Anonimiseren	Anonimiseren is het uitvoeren van datatransformaties zodat de gegevens op geen enkele manier meer tot individuen te herleiden zijn. De richtlijn Test Data Anonimisering gaat dieper in op anonimisering en verschillende niveau's van pseudonimisering.
Applicatieprogrammatuur	Dit zijn alle systemen die de bedrijfsprocessen van UWV ondersteunen, inclusief eventuele beheerconsoles.
Bijzondere gegevens	De AVG onderscheidt bijzondere categorieën van persoonsgegevens, opgenomen in art.9 AVG "Verwerking van bijzondere categorieën van persoonsgegevens". Dit betreft verwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid .

BSO/Securityfunctie divisie	De BSO is de Business Security Officer van de divisie. In de praktijk kan de BSO ervoor kiezen dat de coördinator IB&P de rol van BSO waarneemt.
Geverifieerd	Hiermee bedoelen we alle data, O&H-programmatuur en applicaties die via een gecontroleerd proces in de OTAP-omgevingen van UWV zijn ingevoerd: • Productionele data, die in een gangbaar bedrijfsproces zijn ontstaan; • Testdata die volgens de UWV ICT Richtlijn Test Data Anonimisering zijn ontstaan; • Extern ontwikkelde software en O&H-programmatuur die door de CISO zijn beoordeeld en goedgekeurd; • In het voortbrengingsproces tot stand gekomen applicaties.
IDM - identiteitsmanagement	Deze richtlijn volgt de naamgeving in de richtinggevende IV-principes. In de richtinggevende IV-principes is ervoor gekozen om de Nederlandse afkorting IDM te gebruiken. Het gangbare Engelstalige equivalent is Identity and Access Management (IAM). De IAM visie en –beleid vormen het bovenliggende beleid waarmee IAM governance, gebruikersbeheer, authenticatiebeheer, autorisatiebeheer en controle maatregelen worden toegelicht.
IV-Principes, richtlijnen en uitgewerkte richtlijnen	Het IV-team heeft haar ambities voor de komende jaren uitgedrukt in de *Richtinggevende IV-principes en beleid*. De uitspraken van het IV-team zijn in dit document aangeduid als *IV-principes*. De IV-principes drukken het waartoe en het wat uit. De IV-principes zijn vertaald naar IB&P-consequenties in deze richtlijnen. De IB&P-richtlijnen drukken het *wat* uit. In de praktijk heeft de organisatie ook behoefte aan uitgewerkte richtlijnen. Hierin gaan CISO en staande organisatie in op de "hoe-vraag".
Kritieke informatie	Dit zijn door de securityfunctie van de divisie en/of de systeemeigenaar aangewezen gegevens die het functioneren van UWV ernstig kunnen beïnvloeden. Voorbeelden zijn betaalbestanden, mandateringsgegevens of firewall instellingen.
NFW	Niet functionele werkzaamheden. Dit zijn alle *geautoriseerde* werkzaamheden (zoals ontwikkelen, testen, beheer etc.) die nodig zijn om onze IV-systemen te laten functioneren. Hieronder vallen bijvoorbeeld ook werkzaamheden als troubleshooting of live-testen. De feitelijke werkzaamheden van eindgebruikers vallen buiten dit beleid.
Nonga	Niet op naam gestelde accounts, veelal test- of technische account die niet direct aan één natuurlijke persoon zijn toegewezen.
O&H-programmatuur	Ontwikkel- en Hulpprogrammatuur. Dit zijn alle tooling, de Integrated Development omgeving, analyse en hupprogrammatuur die door functioneel beheerders, technisch beheerders of database specialisten (DBA's) worden gebruikt.
Persoonsgegevens	Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.
Pseudonimiseren	een procedure waarmee identificerende gegevens met een bepaald algoritme worden vervangen door versleutelde gegevens (het pseudoniem). Het algoritme kan voor een persoon altijd hetzelfde pseudoniem berekenen, waardoor informatie over de persoon, ook uit verschillende bronnen, kan worden gecombineerd. De richtlijn Test Data Anonimisering gaat dieper in op anonimisering en verschillende niveau's van pseudonimisering

Technische informatie	Alle gegevens (zoals configuraties of eventlogs) die primair gericht zijn op het functioneren van een applicatie of O&H-programmatuur.
UCRA	UWV Controlled Remote Access project (UCRA). Deze oplossing heeft als doel de toegang voor externe medewerkers te reguleren en te beperken. Toegang tot het UWV HRC kan straks alleen via UCRA en dat kan alleen als de autorisatie geregistreerd is in ABS
Verantwoordelijk management	Dit is het lijnmanagement van de divisie waar het proces en/of het systeem onder valt. Afhankelijk van de zwaarte van een besluit is dit veelal een 2e echelon manager. Daar waar een besluit van de directie wordt verlangd, wordt dit expliciet vermeld.
Vertrouwelijkheidsklasse 2 en 3	UWV past een classificatiemodel toe voor beschikbaarheid, integriteit en vertrouwelijkheid. De denk- en werkwijze is beschreven in de instructie toekennen betrouwbaarheid niveaus. De vertrouwelijkheidsklassen van UWV" en de beleidslijn VIP gegevens (van Gegevensdiensten). Denk aan gegevens voor schuldsanering, financiële informatie of bijzondere categorieën van persoonsgegevens zoals bedoeld in artikel 9 AVG. Verlies, onbehoorlijke of onzorgvuldige verwerking van vertrouwelijkheidsklasse 2 gegevens hebben extra negatieve gevolgen voor de betrokkene. Vertrouwelijkheidsklasse 3 gegevens: dit betreffen strikt vertrouwelijk en gevoelige gegevens waarvan onthulling kan leiden tot (in)directe (politieke) schade.

3 Deel I: Richtinggevende IB&P uitspraken OTAP

Hieronder zijn de uitspraken uit het UWV strategie en beleid vertaald naar IB&P-richtlijnen OTAP. In hoofdstuk 3 is daarmee vastgelegd wat vanuit *IB&P-perspectief* toegestaan m.b.t. de OTAP-omgevingen en OTP-regimes.



Het CISO-office heeft de uitspraken per omgeving uitgewerkt in hoofdstukken 4 en de bijlage .

3.1 Richtinggevende uitspraken, algemeen.

In de richtinggevende IV-principes zijn zes uitspraken gedaan die samen de essentie van het IB&P-beleid OTAP weergeven.

3.1.1	**Gegevens worden alleen verstrekt indien de doelbinding is vastgesteld**	**IBB3, IV-principes**
Toelichting	Gegevens van UWV worden alleen verstrekt en verwerkt indien aan de eisen conform de wetgeving is voldaan.	
Rationale	Veel gegevens van UWV kennen een vertrouwelijk karakter. Het verwerken en verstrekken daarvan dient zorgvuldig te gebeuren. De wet heeft hiervoor regels gesteld en UWV heeft afdoende maatregelen getroffen om hieraan tegemoet te komen.	
Implicaties	Bij de meeste NFW is sprake van verwerking, bij (keten)testen kan sprake zijn van verstrekking. In beide gevallen dienen verwerking en verstrekking proportioneel te zijn beveiligd. Bij het verwerken van testdata gelden de volgende regels: • Data die geen kritieke, bedrijfsgevoelige of persoonsgegevens bevat, mogen overal in O, T, A en P verwerkt worden; • Testdata die geen kritieke, bedrijfsgevoelige of persoonsgegevens bevat, mogen overal in O, T en A verwerkt worden • Voor het testen met data, die *geen* persoonsgegevens en/of bedrijfskritische informatie bevatten, zijn geen aanvullende maatregelen noodzakelijk boven het geldende regime. Het inzien van technische informatie voor NFW is toegestaan indien in redelijkheid vaststaat dat de technische informatie geen persoonsgegevens of kritische gegevens bevat. Testen met een kopie van productionele data is in principe niet toegestaan. Dit is alleen toegestaan met passende voorwaarden.: • De test en/of de verwerking waarvoor getest wordt een rechtstreeks verband houdt met het oorspronkelijke doel van de verstrekking; • Bij nieuwe toepassingen of verwerkingen een relevante privacy impact analyse / gegevenseffectbeoordeling (GEB) beschikbaar is; • De test onder een met het P-regime vergelijkbaar beveiligingsbeleid wordt uitgevoerd; • De securityfunctie van de divisie op de hoogte is gesteld van de test; • Vanuit privacy by design en default zal voor de acceptatie-omgeving eerst maatregelen getroffen dienen te zijn om productiegegevens in acceptatieomgevingen te gebruiken, zoals anonimisering en/of pseudonimisering en/of dataminimalisatie en/of maskeren van gegevens. Maatregelen dienen getroffen te zijn om toegang tot de applicatie/gegevens te beperken, logging uit te voeren op activiteiten en verwijderen verwijderen/vernietigen / onherkenbaar maken van gebruikte gegevens. LET WEL: Bij anonimiseren is herleiding naar persoonsgegevens niet meer mogelijk en is dientengevolge de AVG niet van toepassing. Zie voor uitwerking bijlage 2 sjabloon “gebruik van gegevenssets met persoonsgegevens in een acceptatieomgeving”.	

3.1.2	**Opdeling in functionele en technische domeinen**	**A1**, IV-principes
Toelichting	UWV deelt het ICT-landschap in domeinen in	
Rationale	Indeling in domeinen creëert meer overzicht en geeft een eerste mapping op samenwerkingsmogelijkheden en oplossingen elders in de overheid of de markt	
Implicaties	UWV past een onderverdeling naar Ontwikkel, Test, Acceptatie en Productie toe. De OTAP-omgevingen / -zones zijn door de platformleverancier(s) zodanig van elkaar gescheiden dat niet-geautoriseerde communicatie/ verkeerstromen onderling niet mogelijk zijn: • Het uitgangspunt voor gegevensuitwisselingen tussen systemen zijn geautomatiseerde en geteste applicatiekoppelingen; • Bestandsoverdracht tussen OTAP-zones vindt plaats via de managementzone, waarbij bestanden worden gecontroleerd op kwaadaardige software; Uitzonderingen op deze onderverdeling zijn alleen met goedkeuring van de BSO en de verantwoordelijk directeur mogelijk. Afhankelijk van de ernst van de afwijking kan de BSO de verantwoordelijkheid voor diens directeur waarnemen. De afwijking zal aangemeld dienen te worden ter registratie in het afwijkingenregister.	

3.1.3	**Het netwerkmodel is gebaseerd op een Trusted Assets Network**	**TI7**, IV-principes
Toelichting	De bedrijfsbehoefte van UWV vraagt, in combinatie met de strategische uitgangspunten, om een netwerkmodel dat een transparante en toch gecontroleerde (veilige) uitwisseling van informatie ondersteunt.	
Rationale	Het weghalen van netwerkgrenzen vereist een (functionele) virtualisatie of segmentering binnen het netwerk (een netwerk van netwerken) en een consequente toepassing van bescherming dicht tegen / rond de te beschermen informatie, systemen, applicaties en diensten (Assets). Het resultaat wordt aangeduid als Trusted Assets Network.	
Implicaties	De OTAP-omgevingen / -zones zijn door de platformleverancier(s) zodanig van elkaar gescheiden dat niet geautoriseerde communicatie/ verkeerstromen onderling niet mogelijk zijn. Bestandsoverdracht tussen OTAP-zones vindt plaats via de managementzone, waarbij bestanden worden gecontroleerd. Een (directe) communicatie tussen zones van hetzelfde type binnen (de subdomeinen van) één domein is per definitie toegestaan, tenzij dat om (beveiligings)technische redenen niet mogelijk is. Directe communicatie met het domein en de in dat domein gehoste zones / omgevingen van externe partijen is per definitie **NIET** toegestaan.	
	T.b.v. ontwikkelen, (keten)testen en releasewerkzaamheden wordt alleen gebruik gemaakt van bekende en vertrouwde bronnen: • toegepaste software is afkomstig uit een betrouwbare bron en/of in een UWV eigen ontwikkelproces tot stand gekomen; • de risico's bij de inzet van de toegepaste software zijn bekend en gedocumenteerd • de voor testen en ontwikkelen gebruikte gegevens zijn van een bekende en betrouwbaar geachte bron afkomstig.	

3.1.4	**Mutaties op gegevens zijn herleidbaar tot natuurlijke personen**	**IBB15**, IV-principes
Toelichting	Mutaties op [productionele] gegevens zijn herleidbaar tot personen en/of betrouwbaar geachte bronnen. Mutaties die als bulk zijn aangeleverd worden gearchiveerd en de herkomst van deze gegevens wordt eveneens vastgelegd.	

Rationale	Het moet mogelijk zijn om mutaties op [productionele] gegevens te kunnen herleiden in geval van vragen, bezwaren, beroepszaken en dergelijke.
Implicaties	IV-principe IBB15 is primair gericht op de bescherming van primaire gegevens. De inrichting van onze primaire systemen is hierin de eerste bescherming. Het wijzigingen buiten de systemen om is daarmee ongewenst. Ook bij het uitvoeren van niet functionele werkzaamheden, zijn bewerkingen op gegevens herleidbaar tot natuurlijke personen: • Het is bekend welke functionaris testdata heeft geplaatst of aangepast; • Het is bekend welke functionaris en op welke tijdstippen toegang heeft tot kritieke gegevens, systeeminstellingen en/of persoonsgegevens; Direct wijzigen van gegevens, systeeminstellingen en/of persoonsgegevens buiten de productionele systemen of een beheerconsole om is ingevolge deze richtlijn alleen onder bijzondere en uitzonderlijke omstandigheden toegestaan: • Het herstellen van een productieprobleem; • Door één daartoe geautoriseerd functionaris, waarbij het aantal bijzondere toegangen beperkt is; • Indien een controle op de toegang mogelijk is. Dit kan al naargelang de gevoeligheid van de data variëren van een zichtcontrole tot en met een beheerste toegang i.c.m. logging. De BSO beoordeelt de toegang en geeft namens of met divisiedirecteur toestemming voor de toegang. LET WEL: Vanuit privacy by design en default zal voor het testen met productiegegevens anonimiseren of pseudonimiseren het uitgangspunt moeten zijn. Het testen met productiedata is in principe niet toegestaan. Testen met productiedata is met specifieke voorwaarden in uitzonderlijke situaties toegestaan waarbij extra maatregelen dienen te zijn getroffen. Gestelde voorwaarden om toegang tot productieomgeving te verschaffen t.b.v. testen in geval van uitzonderlijke omstandigheid: • Er is geen ander realistisch alternatief voor testen met productiedata; • De test dient een directe business case of in ieder geval een bedrijfsbelang; • Risico's m.b.t. de test zijn in overleg met de securityfunctie van de betrokken divisie(s) beheerst; • De test vindt onder een met het P-regime vergelijkbare beveiliging plaats; • De directie neemt de verantwoordelijkheid voor de test; • Met het oog op wettelijke rechten van betrokkenen is de gang van zaken aantoonbaar gedocumenteerd t.a.v. noodzaak tot verwerving en verwerking en getroffen maatregelen; • Maatregelen dienen getroffen te zijn om toegang tot de applicatie/gegevens te beperken, logging uit te voeren op handelingen en het verwijderen/vernietigen / onherkenbaar maken van gebruikte gegevens; • De test set wordt zo snel mogelijk na gebruik verwijderd. Zie voor uitwerking bijlage 2 sjabloon "gebruik van gegevenssets met persoonsgegevens in een acceptatieomgeving"
	Opmerking. Onder "aanpassen" van testdata valt ook het verwijderen van testsets. Vanuit IB&P-optiek is de verwijdering van testdata vereist als sprake is van persoonsgegevens. Hierbij moet de organisatie nadenken over een eventuele archivering, maar dit valt verder buiten de IB&P-richtlijnen.

3.1.5	**Van elk gegeven is bekend waar de laatste actuele versie is**	**VG10**, IV-principes
Toelichting	Van sommige gegevens ontstaat een serie opeenvolgende waarden in diverse registraties. Van belang is om op elk moment het juiste gegeven te kunnen reproduceren. Basis is in ieder geval het UWV-brede CGM/UGR	
Rationale	Zowel binnen UWV als binnen de overheid kunnen meerdere versies van dezelfde gegevens voorkomen. Voor het informeren en bewerken van deze gegevens is het noodzakelijk dat bekend is waar de laatste versie van een gegeven (binnen of buiten UWV) bekend is	
Implicaties	Testen mag niet leiden tot (onbedoelde)mutatie van primaire gegevens. Testen met productionele systemen is in principe niet toegestaan. Indien echter de noodzaak daartoe bestaat om te testen met productiedata dienen maatregelen getroffen te zijn en zijn daarmee onder zeer specifieke voorwaarden toegestaan: a. Voor "go-live" testen; b. Indien geen ander realistisch alternatief voor testen met een productiesysteem voorhanden is. In beide gevallen is aan de navolgende condities voldaan: c. De (keten)test dient een businessrationale en/of heeft een positieve business case; d. Maatregelen zijn getroffen die onbedoelde waarneming of verwerking van gevoelige, kritieke of persoonsgegevens tegengaan; e. De gegevens- en/of systeemeigenaar zijn formeel en schriftelijk op de hoogte gebracht van de test en per test; f. Maatregelen zijn getroffen die onbedoelde mutatie van productiedata tegengaat; g. Indien de testdata eenvoudig herkenbaar en eenvoudig uit de primaire systemen te verwijderen is h. Met het oog op wettelijke rechten van betrokkenen is de gang van zaken aantoonbaar gedocumenteerd t.a.v. noodzaak tot verwerving en verwerking en getroffen maatregelen; i. Vanuit privacy by design en default zal voor het testen met productiegegevens anonimiseren of pseudonimiseren het uitgangspunt moeten zijn en dienen maatregelen getroffen te zijn om productiegegevens te gebruiken in testtrajecten, zoals anonimisering en/of pseudonimisering en/of dataminimalisatie en/of maskeren van gegevens; j. Maatregelen dienen getroffen te zijn om toegang tot de applicatie/gegevens te beperken, logging uit te voeren op handelingen en het verwijderen/vernietigen / onherkenbaar maken van gebruikte gegevens; k. De securityfunctie van UWV en de betrokken systeem/gegevenseigenaar hebben de werkwijze expliciet toegestaan. De betrokken BSO's hebben na consultatie van de centrale security functie de IB&P-risico's beoordeeld. De directie van de divisie (dan wel hun BSO) heeft de test toegestaan. LET WEL: Bij anonimiseren is herleiding naar persoonsgegevens niet meer mogelijk en is dientengevolge de AVG niet van toepassing. . Het kan in bepaalde omstandigheden nodig zijn om met een kopie van primaire gegevens te werken. Een voorbeeld is bijvoorbeeld het naspelen van verstoringen. Dit zal met maatregelen geborgd moeten worden zoals beperkte groep van gebruikers, omgeving beperkt toegankelijk, logging, verwijderen gegevens na gebruik, etc…	
Opmerking	De IB&P-implicatie is voornamelijk gericht op de bescherming van de primaire systemen en -registraties. Uiteraard kan het bij testen noodzakelijk zijn om verschillende soorten datasets te gebruiken. Denk bijvoorbeeld aan regressietesten. Ook hier moet de organisatie weten welk gegeven op welk moment en plaats is gebruikt. Zolang dit géén persoons- or primaire gegevens zijn, is dit echter geen IB&P-issue. Bij het uitvoeren van regressietesten is het noodzakelijk om testsets aan te passen. Uiteraard vereist goed testen een goed versiebeheer, maar vanuit IB&P-oogpunt is dit toegestaan.	

3.1.6	**De integriteit en vertrouwelijkheid van informatie is gewaarborgd**	**IBB6**, IV-principes
Toelichting	De richtlijnen voor de integriteit en vertrouwelijkheid van informatie worden bepaald door het Tactisch Beleid Beveiliging & Privacy van UWV.	
Rationale	Informatiebeveiliging, privacy, fysieke beveiliging en persoonsbeveiliging zijn de vier basisdisciplines van Beveiliging & Privacy. Informatiebeveiliging beschrijft de maatregelen voor het waarborgen van de juiste beschikbaarheid, integriteit en vertrouwelijkheid (exclusiviteit).	
Implicaties	Tactisch Beleid Beveiliging & Privacy UWV streeft ernaar de P-omgevingen en P-regimes zo vorm te geven dat: • Gegevens beschermd zijn tegen onbevoegde waarneming en dat hierbij is uitgegaan van vertrouwelijkheidsklasse 2; • Gegevens beschermd zijn tegen onbedoelde wijziging; • Wijzigingen aan gegevens tot natuurlijke personen of concrete acties zijn herleidbaar. Dit doet UWV door maatregelen op proces-niveau, op persoonsniveau, technische maatregelen en risicoafweging. Op persoonsniveau zorgen de maatregelen ervoor dat: • alleen daartoe geautoriseerde medewerkers toegang hebben tot de systemen; • werkzaamheden herleidbaar zijn tot individuele medewerkers; • functionarissen gebonden zijn aan een geheimhoudingsverklaring. Op procesniveau zijn: • beheerprocessen beschreven en vastgesteld; • de gebruikte O&H-programmatuur is bekend en eventuele risico's bij het gebruik van de O&H-programmatuur zijn beheerst; Op technisch niveau: • Is het UWV op netwerkniveau afgescheiden van de buitenwereld door een samenhangend stelsel van gangbare beveiligingsoplossingen zoals DMZ, anti-DDoS, anti-Malware. Bij de beoordeling of een techniek gangbaar is, baseert UWV zich op de stand der techniek; • gaat UWV uit van een standaard configuratie voor netwerkcomponenten en servers, inclusief een hardeningsbeleid; • Zijn alle koppelingen bekend, gebaseerd op een businesscase, beheerd en beveiligd. hierbij heeft UWV de ambitie dat alle gegevensverbindingen cryptografisch beveiligd zijn en het zero-trust beginsel hanteren; • Het toepassen van encryptie voor datasets, databases of verbindingen is een overweging, mits dit de beveiliging of stabiliteit van UWV niet ondergraaft. • Acceptatieomgevingen vallen ook onder het P-regime. Aanvullend geldt ten aanzien van verwerking van persoonsgegevens dat vanuit privacy by design en default voor het testen met productiegegevens anonimiseren of pseudonimiseren het uitgangspunt moet zijn en dienen maatregelen getroffen dienen te zijn als productiegegevens in acceptatieomgevingen worden gebruikt, zoals anonimisering en/of pseudonimisering en/of dataminimalisatie en/of maskeren van gegevens. Tevens dienen maatregelen getroffen te zijn om toegang tot de applicatie/gegevens te beperken, logging uit te voeren op handelingen en verwijderen/vernietigen / onherkenbaar maken van gebruikte gegevens. LET WEL: Bij anonimiseren is herleiding naar persoonsgegevens niet meer mogelijk en is dientengevolge de AVG niet van toepassing. Zie voor uitwerking bijlage 2 sjabloon "gebruik van gegevenssets met persoonsgegevens in een acceptatieomgeving" In de risico afweging zijn doelbinding, proportionaliteit en risico's bij de verwerking door de BSO beoordeeld.	

3.1.7	**Beveiligingsmaatregelen zijn gebaseerd op risicoklassen**	**IBB8**, IV-principes
Toelichting	De gekozen beveiligingsmaatregelen ter bescherming van de betrouwbaarheidsaspecten integriteit en vertrouwelijkheid zijn minimaal van vertrouwelijkheids- en integriteitsklasse 2.	
Rationale	De risico's voor integriteit en vertrouwelijkheid worden aangeduid in risicoklassen. UWV heeft risicoklassen gedefinieerd voor het waarborgen van integriteit en vertrouwelijkheid in haar UWV BZ BIV classificatierichtlijn.	
Implicaties	De in de IB&P-richtlijnen OTAP benoemde regimes zijn maximaal gericht op vertrouwelijkheidsklasse 2, beschikbaarheidsklasse 2 UWV en integriteitsklasse 2 UWV. Om eenvoud en beheerbaarheid in het UWV landschap te bereiken, worden lagere klassen op een zelfde manier behandeld. Verwerking van lagere vertrouwelijkheids- en integriteitsklassen is toegestaan en de beveiligingsmaatregelen worden toereikend geacht; De verantwoordelijke directie vergewist zich of aanvullende maatregelen nodig zijn. Bij nieuwbouw of grotere aanpassingen stelt de directie met de securityfunctie vast of classificaties, risico-inschattingen aangepast moeten worden. Het kan nodig zijn om voor deze risico-inschattingen, een gegevenseffectbeoordeling (GEB) (voorheen een Privacy Impact Analyse (PIA)) en/of een Business IB&P Requirementsanalyse (BIRA) uit te voeren. Indien hogere eisen gesteld worden, overweegt de organisatie de inzet van aanvullende maatregelen, zoals: • Een afgeleide medische geheimhouding bij de verwerking van medische gegevens; • Toepassen van technieken zoals redundantie bij zeer kritische processen. De security functie van de divisie (BSO) is betrokken in deze overweging.	

3.2 Uitspraken m.b.t. inrichting van beheer en de verantwoordelijkheden

3.2.1	**Beheer- en ontwikkelprocessen zijn formeel vastgelegd**	**IBB12**, IV-principes
Toelichting	Daar waar oplossingen van verschillende leveranciers worden ingezet en veel nieuwe producten of diensten worden ingezet, is het behouden van een uniforme omgeving steeds moeilijker.	
Rationale	Beheerprocessen dienen formeel te zijn vastgelegd, met duidelijke afspraken over verantwoordelijkheden en koppelvlakken.	
Implicaties	De verantwoordelijkheden bij niet-functionele werkzaamheden zijn als volgt: • De directie is eindverantwoordelijk m.b.t. risico-inschattingen en risico-acceptatie. De securityfunctie van de divisie is hierin adviserend; • De ontwikkelende (of testende) partij stelt met de beheerpartij vast of de standaard hulpmiddelen (ontwikkel-, testomgeving en ondersteunende systemen) volstaan en of UWV risico's loopt bij het gebruik van de O&H-programmatuur; • Afwijkingen van de standaard O&H-programmatuur en werkwijze worden beoordeeld door de securityfunctie en geregistreerd door het USOC. Grotere risico's worden door de directie geaccepteerd, anders volstaat het oordeel van de securityfunctie van de divisie. • Het lijnmanagement is verantwoordelijk voor de inrichting van en de controle op de beheerprocessen. Beheerwerkzaamheden zijn expliciet beschreven: • Werkzaamheden, het doel en de aard van de niet functionele werkzaamheden; • Geraakte objecten en data, waarbij een duidelijk onderscheid is gemaakt tussen testdata, systeeminstellingen, kritieke informatie of persoonsgegevens; • De gebruikte O&H-programmatuur, en hoe deze O&H-programmatuur is ingezet; • De noodzakelijke acties en welke partij verantwoordelijk is voor de acties	

3.2.2	**De beheerder van gegevens waarborgt de integriteit van en geautoriseerde toegang tot de gegevens**	**IBB13**, IV-principes
Toelichting	Juist en geautoriseerd gebruik van gegevens wordt bewaakt door de beheerder van die gegevens.	
Rationale	Het uitvoeren van NFW kan onbedoelde gevolgen hebben. Directe benadering van gegevens kan tot aanpassing van autorisaties leiden. Ook het wijzigen van gegevens buiten de applicatie om kan tot integriteitproblemen leiden. Beheer is noodzakelijk om een juiste en integere registratie te kunnen voeren voor zo lang als dit in het kader van verantwoording en de recht- en bewijszoekende burger noodzakelijk is.	
Implicaties	Ook bij het uitvoeren van niet-functionele werkzaamheden is de systeemeigenaar verantwoordelijk voor het blijvend functioneren van de beheerde applicaties: • De systeemeigenaar richt de beheerprocessen voor zijn systeem in; • De directie van de divisie is eindverantwoordelijk; • De securityfunctie van de divisie is adviserend naar de systeemeigenaar of de directie; • De systeemeigenaar vergewist zich ervan of de verwerker die technisch beheer voor haar rekening neemt (partij aan wie de ICT/software/beheer is uitbesteed) passende maatregelen heeft getroffen die een passend beveiligingsniveau garanderen. De systeemeigenaar zorgt ervoor dat 1) Niet-functionele werkzaamheden vooraf zijn gedefinieerd 2) Voordat O&H-programma's worden ingezet, zijn de risico's ten aanzien van stabiliteit & continuïteit en IB&P afgewogen; Processen en instructies zorgen ervoor dat werkzaamheden correct en volgens afspraken worden uitgevoerd. Streven hierbij is dat de onder 2 gesignaleerde risico's technisch en/of procedureel zijn afgedekt.	
Opmerking	Dit is een operationele invulling van IBB12.	

3.3 Uitspraken m.b.t. communicatie en toegang

De regels voor gegevensuitwisselingen in en tussen regimes zijn een nadere uitwerking van IV-principe A1 uit de richtinggevende IV-principes. In de IB&P-richtlijnen OTAP onderscheiden we:

- (geautomatiseerde) gegevensuitwisseling tussen systemen;
- Software distributie;
- Bestandsuitwisseling (standaard en éénmalig).

3.3.1	**Communicatie tussen services verlagen het beveiligingsniveau niet**	**IBB16**, IV-principes
Toelichting	Bij gegevensverkeer tussen services worden afdoende maatregelen getroffen rekening houdende met de risicoklasse van de gegevens	
Rationale	Communicatie tussen services mag geen beveiligingslek of verstoring van het primaire proces opleveren:	
Implicaties	Services zijn dermate geconstrueerd en/of afgeschermd dat deze geen nieuw beveiligingsissue opleveren. Productionele koppelingen zijn geautoriseerd, via een gecontroleerd voortbrengingsproces ontwikkeld en getest. Waar mogelijk en doenlijk zijn koppelingen gebaseerd op het *zero-trust* [3]principe: • Koppelingen zijn zo ingericht dat ze alleen verkeer accepteren dat afkomstig is van een bekende node. Authenticatie op basis van certificaten heeft hierbij de voorkeur; • Koppelingen zijn opgezet vanuit het "default deny"-principe. Alleen geauthenticeerde of geautoriseerde handelingen worden in principe ondersteund. Een afweging zal moeten gemaakt worden op basis van een risico-afweging t.b.v. bruikbaarheid en veiligheid . Het eerste aanloggen, het initiëren van een communicatieprotocol of het benaderen van openbare bronnen zijn voorbeelden van wel geautoriseerde acties.	

3.3.2	**Communicatie met derden volgens vastgestelde standaarden**	**AE12**, IV-principes
Toelichting	UWV past de standaarden toe die gelden binnen de Overheid en zijn vastgesteld door het College Standaardisatie en maakt gebruik van het 'pas toe of leg uit' principe van de Overheid	
Rationale	Bij (elektronische) communicatie moet altijd duidelijk zijn wat bedoeld wordt met de gecommuniceerde gegevens. Standaardisatie voorkomt begripsverwarring	
Implicaties	UWV streeft ernaar om courante versies van beveiligingsprotocollen en -inzichten toe te passen. Het toepassen van een oudere werkwijze is mogelijk: • Als gedocumenteerde exceptie; • Op basis van een aanwijsbaar bedrijfsvoordeel of een duidelijke business case; • Indien dit geen onoverkomelijke risico's voor UWV oplevert; • Indien geen moderne oplossingsstrategie beschikbaar is.	

3.4 Uitspraken m.b.t. Identiteitsbeheer in niet-functionele werkzaamheden

3.4.1	**IDM (Identitymanagement) is een UWV-brede voorziening**	**IG1**, IV-principes
Toelichting	IDM is een UWV-brede voorziening die waarborgt dat handelingen zijn te herleiden naar natuurlijke personen. Daar waar mogelijk wordt aangesloten op federatieve stelsels.	
Rationale	Een integrale informatievoorziening gedraagt zich voor gebruikers als één geheel, waardoor Single Sign-on mogelijk is en er, door het ontbreken van interne grenzen geen (of minder), kans op de 'wrong door' is.	
Implicaties	Waar mogelijk en realistisch, wordt voor alle toegang (inclusief NFW) gesteund op de standaardoplossingen: • Registratie van de betrokken functionarissen en hun rechten vindt plaats in ABS; • Feitelijke toegang wordt verleend via UCRA; • Als provisioning via Active Directory mogelijk is, heeft dit de voorkeur Afwijkingen zijn alleen gemotiveerd mogelijk, op basis van een risicoanalyse en met toestemming van de securityfunctie van UWV en vastlegging in een riskletter en/of afwijkingenregister.	

3.4.2	**IDM leidt handelingen terug tot natuurlijke personen**	**IG2**, IV-principes
Toelichting	Single Sign-on en het herleiden van handelingen naar natuurlijke personen is mogelijk door gestandaardiseerde koppelingen tussen administraties binnen het UWV IDM.	
Rationale	Bij Single Sign-on logt de gebruiker slechts eenmalig in om op andere systemen geauthenticeerd te zijn. Dit is mogelijk als de andere systemen de authenticatie vertrouwen van het systeem, waarop de gebruiker zich authentiseert.	

Implicaties	Het uitvoeren van NFW is herleidbaar tot natuurlijke personen. Indien de standaard voorzieningen als toegang via Extranet en UCRA voor externe medewerkers geschikt zijn, verdient dit de voorkeur. Toegang buiten de standaard UWV voorzieningen is dus alleen mogelijk indien:
	• Dit een goedgekeurde en gedocumenteerde afwijking is;
	• De gebruikersorganisatie zelf maatregelen treft om herleidbaarheid te borgen:
	  ○ De teammanager is verantwoordelijk voor een registratie van gebruik;
	  ○ De registratie is op persoonsniveau;
	  ○ De teammanager controleert of de registratie juist en volledig is.
	Uiteraard kan de teammanager steunen op bestaande oplossingen zoals de KA-inlog.	

3.4.3	**Autorisaties zijn gebaseerd op het RBAC-model**	**IBB14**, IV-principes
Toelichting	Autorisaties worden formeel uitgegeven en gebaseerd op RBAC (Role Based Access Control).	
Rationale	Autorisatie is het proces waarin personen of processen rechten krijgen op het benaderen van een bestand of een systeem. De autorisatie wordt aan een rol toegekend door de eigenaar van het object. Het meest gebruikte principe daarbij is need-to-know: je mag alleen zien wat je voor je functie nodig hebt.	
Implicaties	De toegang tot systemen, hulpbronnen en O&H-programmatuur is gebonden aan de uit te voeren niet-functionele werkzaamheden. De voor NFW verleende toegang is zo mogelijk beperkt tot technische informatie. Indien Persoonsgegevens in geding zijn, geldt 3.1.1 (IBB3) en 3.4.2 (IG2)	

3.5 Infrastructurele principes m.b.t. NFW-OTAP

3.5.1	**Infrastructuur dient gestandaardiseerd te worden**	**I1**, IV-principes
Toelichting	Standaardisatie van de infrastructuur moet worden nagestreefd.	
Rationale	Een onnodige verscheidenheid in de infrastructuur, het fundament van de informatiehuishouding, verhoogt de complexiteit en de kosten, onder andere omdat er meer kennis opgebouwd en onderhouden moet worden. Standaard componenten lenen zich eveneens beter voor hergebruik	
Implicaties	De IB&P-richtlijnen volgen de algemene beleidsprincipes *eenvoud* en *testbaarheid*: • Voor ontwikkel- en testwerkzaamheden, wordt gebruik gemaakt van een integrated development (IDE) omgevingen. Hierbij streeft UWV naar uniformiteit en beheersbaarheid; • Uit het oogpunt van testbaarheid, zullen O&H-programmatuur en rechten voor functionele werkzaamheden zijn afgeleid van de technisch beheerders in het productieregime. Dit voorkomt dat ontwikkelaars onbewust oplossingen kiezen die in productie niet werken; • Vanuit het oogpunt van standaardisatie is O&H-programmatuur in T en A (voor niet-functionele werkzaamheden) zoveel mogelijk gelijk aan de O&H-programmatuur in de P-omgeving. Afwijking van deze aanpak is de keuze van het verantwoordelijk management*), in overleg met de securityfunctie*) In de keuze weegt het management tenminste kosten, compatibiliteit met de productieomgeving, security- en stabiliteit & continuïteitsrisico's en beheerbaarheid af.	

3.5.2	**Geautomatiseerde deployment van software en configuraties**	**IBB2**, IV-principes
Toelichting	Configuratiemanagement, het verzamelen, registreren en gebruiken van configuratiegegevens, ondersteunt de beheerder door de configuratiegegevens buiten de systemen / voorzieningen op te slaan.	
Rationale	Een (geautomatiseerde) deployment van software en configuratiegegevens vermindert de (manuele) beheerinspanning bij infrastructuurcomponenten die reeds zijn geïnstalleerd.	
Implicaties	Waar relevant (en rationeel) zijn de volgende richtlijnen van toepassing:	

	• Beveiligingsinstructies m.b.t. applicatie ontwikkeling, inclusief spelregels voor het (her)gebruik van bekende en beproefde componenten zijn opgenomen in SSD; • Software update wordt automatisch gedeployed volgens Audio; • Software en configuraties is hardeningsbeleid

4 Deel II: IB&P-richtlijnen per OTAP-regime

De implicaties uit de IV-principes en het IV-beleid zijn in dit hoofdstuk kort vertaald naar concrete werkzaamheden. Per regime (of in een enkel geval per omgeving) zijn de toegestane NFW opgenomen. Om een doublure in beschrijvingen te voorkomen, zijn de werkzaamheden per keer beschreven in de bijlage.

4.1 IB&P uitspraken voor het P-regime

Onder het P-regime vallen zowel de productie als de acceptatieomgevingen indien deze onder beheer van het datacenter staan. Doel van het P-regime is het bieden van een stabiele, beveiligde omgeving waarin vertrouwelijkheidsklasse 2 gegevens conform de UWV eisen verwerkt kunnen worden. Dit veronderstelt dat alleen met geverifieerde applicaties, O&H-programmatuur en data wordt gewerkt.
Het P-regime dient voor het ondersteunen van bedrijfsprocessen. Om de continuïteit van het primaire proces te borgen, kan de organisatie een A-omgeving inrichten onder het P-regime, vallend onder dezelfde voorwaarden als de Productie-omgeving. De A-omgeving ontlast de P-omgeving bij het doen van stress-, load- of acceptatietesten.

Binnen het P-regime zijn de volgende niet-functionele werkzaamheden toegestaan:.

- Het inzien en plaatsen van configuratiebestanden. Hieronder valt ook het via een vooraf afgesproken werkwijze raadplegen van eventlogs;
- Het uitvoeren van een pre-productietest ten behoeve van 'live'-gang;
- Het incidenteel en ongepland inzien van configuratiebestanden via een noodprocedure *(het ten behoeve van NFW via UCRA benaderen van het P-regime door externen conform de ontheffingsprocedure CSD/ Handreiking Red envelop controlled access procedure);*
- Het incidenteel en ongepland uitvragen van productiegegevens indien de noodzaak daartoe aantoonbaar bestaat en onderbouwd kan worden met een risico-analyse, onder de volgende voorwaarden:
    - De securityfunctie van UWV en de betrokken systeem/gegevenseigenaar hebben de werkwijze expliciet toegestaan. De betrokken BSO's hebben na consultatie van de centrale security functie de IB&P-risico's beoordeeld en vastgelegd. De directie van de divisie (dan wel hun BSO) heeft de toegang toegestaan.
    - de uitvraag vindt strikt gecontroleerd plaats.
    - de uitvraag van productie data is bedoeld om een structurele oplossing voor een urgent probleem te realiseren.
    - de gang van zaken is aantoonbaar gedocumenteerd t.a.v. noodzaak tot verwerving en verwerking en getroffen maatregelen.
    - Maatregelen dienen getroffen te zijn om toegang tot de applicatie/gegevens te beperken en logging dient plaats te vinden op uit te voeren activiteiten.
    - aantoonbaar vernietiging van eventuele kopie productiegegevens direct na gebruik.

Als voorbeeld een incidentonderzoek dat niet op een andere manier dan in de productie-omgeving kan plaatsvinden

De noodzaak en de beveiligings- en privacyrisico's moeten afgewogen en vastgelegd zijn, passende mitigerende maatregelen moeten ingericht zijn en een aantoonbaar akkoord hebben van de Business Security Officer (BSO).

Voor de Acceptatie-omgeving zijn er binnen het P-regime de volgende aanvullende werkzaamheden toegestaan:

- Het anonimiseren of pseudonimiseren van data ten behoeve van het overbrengen van deze data naar de acceptatieomgeving onder het P-regime;
- Het anonimiseren van data ten behoeve van het overbrengen van deze data naar de testomgeving onder het T-regime*;*
- Stress en load testen, met niet-persoonsgebonden accounts, onder de voorwaarden:
  - Herleidbaar is wie de NONGA gebruikt;
  - Gebruik is op auditeerbare wijze vastgelegd;

  zie de voorwaarden van NONGA-gebruik voor testdoeleinden (IB&P richtlijn NONGA);
- Gebruikersacceptatietesten, in bijzondere gevallen met niet-persoonsgebonden accounts, onder de voorwaarden:
  - Herleidbaar is wie de NONGA gebruikt;
  - Gebruik is op auditeerbare wijze vastgelegd;

  zie de voorwaarden van NONGA-gebruik (IB&P richtlijn NONGA);
- Testen en aanpassen van configuratiebestanden ten behoeve van de Productie-omgeving;
- Evalueren van software stacks en patches;
- meekijken in accounts op de database via de red envelop procedure;
- Smoke test (kleinschalige test om functioneren van een koppeling vast te stellen).

LET WEL: Bij anonimiseren is herleiding naar persoonsgegevens niet meer mogelijk en is dientengevolge de AVG niet van toepassing.

Op bovenstaande punten is uitgangspunt privacy by design en default voor het geanonimiseerd of gepseudonimiseerd testen met productiegegevens. Maatregelen dienen getroffen te zijn op:

- geminimaliseerd data gebruik,
- beperkte toegang tot de applicatie/gegevens,
- logging uitvoeren op activiteiten,
- verwijderden/vernietigen / onherkenbaar maken van de gebruikte gegevens.

De noodzaak en de beveiligings- en privacyrisico's moeten afgewogen en vastgelegd zijn. Passende mitigerende maatregelen moeten ingericht en vastgelegd zijn in overleg met de Business Security Officer.

De volgende werkzaamheden zijn onder het P-regime ongewenst. Een uitzondering is alleen mogelijk met toestemming van de systeemeigenaar en de BSO gezamenlijk, voorzien van een risico-analyse, danwel impact analyse:

- Het live patchen in een P-*omgeving*, zonder dat de patch in de A-omgeving is getest. Onder bijzondere omstandigheden kan het noodzakelijk zijn een patch door te voeren, zonder dat deze voldoende getest is.

De volgende werkzaamheden zijn onder het P-regime in principe verboden. Een uitzondering kan alleen toegestaan worden door de systeemeigenaar, de securityfunctie en de directie van de divisie gezamenlijk, voorzien van een vastgelegde risico-analyse, danwel impactanalyse.

- Het aanpassen van programmatuur in een P-*omgeving*, zonder dat de aangepaste software in een A-omgeving is getest.

Het lijnmanagement is zelf verantwoordelijk voor toezicht op de goede uitvoering van de werkzaamheden:

- De uitvoerder van de NFW (projectmanager of lijnmanagement functioneel beheer) houdt toezicht op de werkzaamheden, registreert eventuele uitzonderingen en verantwoordt zich hierover aan de systeemeigenaar en/of de BSO;
- Het lijnmanagement bewaakt samen met de BSO de trends en gaat na of aanvullende acties (uitzetten verbeteracties, aanvragen beleidsaanpassing etc.) noodzakelijk zijn.

NOOT:
In de IB&P-richtlijnen OTAP is uitgegaan van de baseline voor UWV. De baseline van UWV zorgt ervoor dat binnen heel UWV tot en met vertrouwelijkheidsklasse 2 (beleid UWV BZ BIV classificatie) data gewerkt kan worden. Dit is geregeld door een combinatie van procedures, geheimhoudingsverklaringen, technische maatregelen en dergelijke.

De implicatie is dat zolang aan de voorwaarden in het IB&P-beleid OTAP wordt voldaan, de onderstaande werkzaamheden bijvoorbeeld toegestaan zijn in het P-regime.

1. Waarnemingen van bestanden met gebruikersinformatie om problemen te diagnosticeren. De waarneming vindt namelijk o.b.v. de oorspronkelijke verwerking plaats (doelbinding) en voor de onderzoekende functionaris gelden dezelfde voorwaarden als in de productieomgeving (geheimhouding, tooling). De waarneming blijft beperkt tot een zo klein mogelijke dataset.
2. Het inzien van eventlogs om de juiste werking van systemen vast te stellen of om problemen op te lossen. Dit is geen probleem, zolang de eventlogs alleen technische informatie of hoogstens een username bevatten. (Een username is vertrouwelijkheidsklasse 1, dus dit valt onder de baseline).

4.2 IB&P uitspraken voor het T-regime

Onder het T-regime vallen de T-omgevingen. Dit zijn bijvoorbeeld zowel de hosted T-omgevingen als OToD. Doel van het T-regime is het functioneel testen van opgeleverde software. De T-omgevingen zijn logisch afgescheiden van de omgevingen die onder het P-regime vallen. Dit maakt het mogelijk om meer en krachtiger O&H-programmatuur in te zetten. Hier staat tegenover dat het toepassen van ontwikkeltooling alleen onder strikte voorwaarden mag worden toegepast: voorkomen moet worden dat niet gedocumenteerde software in het voortbrengingsproces wordt geïntroduceerd.

De volgende NFW zijn onder het T-regime toegestaan:

- Het onder (configuratie)beheer plaatsen, aanpassen en verwijderen van de te testen applicatiesoftware;
- Het plaatsen, aanpassen en verwijderen van testdata;
- Directe toegang met CRUD rechten tot de testdatabase;
- Het toepassen van speciale hulpprogrammatuur om software kwaliteit te testen;
- Het toepassen van speciale hulpprogrammatuur om kwetsbaarheden in applicaties te toetsen.

De volgende werkzaamheden zijn onder het T-regime verboden.

- Het aanpassen van applicatieprogrammatuur. Onder bijzondere omstandigheden kan het noodzakelijk zijn een noodfix door te voeren, maar deze moet herleidbaar zijn naar de ontwikkelomgeving en/of ontwikkelaar. Een uitzondering kan alleen verleend worden door de ontwikkelende en beherende partij gezamenlijk. De ontvangende IV-organisatie –inclusief de BSO- moet (z.s.m. en eventueel naderhand) van de aanpassingen op de hoogte worden gebracht.
- Testen of ontwikkelen met data dat niet geanonimiseerd/gepseudonimiseerd is.

4.3 IB&P uitspraken voor het O-regime

Onder het O-regime vallen de O-omgevingen. Dit zijn zowel de hosted O-omgevingen, OToD als ontwikkelomgevingen bij de applicatiebouwer. Doel van het O-regime is het (gecontroleerd) opleveren van software. De O-omgevingen *en in het bijzonder de daarop aanwezige tooling* zijn onderscheiden en waar mogelijke afgescheiden van omgevingen die onder het P-regime vallen. Dit maakt het mogelijk om meer en krachtiger O&H-programmatuur in te zetten. Hier staat tegenover dat het gebruiken van persoonsgegevens of kritieke data niet is toegestaan. De veelheid aan nieuw ontwikkelde software betekent dat data uit de O-omgeving onbedoeld kan worden doorgeleverd.

De volgende NFW zijn onder het O-regime toegestaan:

- Het onder configuratiebeheer plaatsen, aanpassen en verwijderen van de te testen applicatiesoftware;
- Het plaatsen, aanpassen en verwijderen van geanonimiseerde testdata;
- Het toepassen van speciale hulpprogrammatuur om software kwaliteit te testen;
- Het toepassen van speciale hulpprogrammatuur om kwetsbaarheden in applicaties te toetsen.

De volgende werkzaamheden zijn onder het O-regime verboden.

Testen of ontwikkelen met gepseudonimiseerde data waarbij herleiding naar personen mogelijk blijft.

Bijlage: Beschrijving niet-functionele werkzaamheden

Om doublure in beschrijvingen te voorkomen, zijn alle onderkende werkzaamheden hieronder eenmalig beschreven.

OTAP-G01	**Inzien en plaatsen configuratiebestanden**	**Richtlijn**
Doel	Controleren en eventueel aanpassen van configuratiesettings die niet via ESA kunnen worden uitgerold, danwel hersteld moeten worden.	
Geldigheid	Alle regimes (P, T, O)	
Wie	Door UWV aangewezen functionarissen. Alleen daartoe aangewezen en opgeleide medewerkers van UWV, hosting provider en/of applicatiebouwer mogen deze werkzaamheden uitvoeren.	
O&H-programmatuur	*Zie UCRA/RDT-richtlijn*	
Voorwaarden	Werkzaamheden zijn onder de volgende voorwaarden toegestaan: 1) De uitvoerende functionarissen zijn a) gehouden aan een geheimhoudingsverklaring; b) bekend met hun werkzaamheden en O&H-programmatuur. 2) De te gebruiken O&H-programmatuur en werkzaamheden zijn beschreven, de risico's m.b.t. IB&P en stabiliteit & continuïteit zijn bekend en de risico's zijn afgehandeld. 3) De functionarissen werken met een persoonsgebonden toegang, zodat herleidbaar is wie op welk moment een beheerderstoegang heeft gebruikt. 4) De organisatie weet wie kritieke handelingen heeft uitgevoerd: a) De systeemeigenaar wijst kritieke handelingen aan. Dit zijn bijvoorbeeld aanpassen van stamtabellen, het muteren van betaalbestanden of het inzien van beveiligingsinstellingen; b) In traceerbaarheid kan worden voorzien door combinatie van de KA-inlog, in combinatie met een logboek van de kritieke handelingen.	xxx IDM1 tm IDM 4

OTAP-G02	**Red envelop controlled acces procedure**	**Richtlijn**
Doel	Het bieden van een gecontroleerde toegang voor externe functionarissen voor het uitvoeren van NFW.	
Geldigheid	P-regime (P en A omgevingen binnen IBM omgeving onder P maatregelen).	
Wie	Door één van onze leveranciers aangewezen, met naam bekende functionarissen. Alleen daartoe aangewezen en geautoriseerde medewerkers van UWV, hosting provider en/of applicatiebouwer mogen deze werkzaamheden uitvoeren.	
Gekoppelde richtlijnen	Richtlijnen OTAP, richtlijnen remote desktop toegang (RDT), handreiking Red envelop controlled access procedure	
O&H-programmatuur	Remote desktop connection procedure (RDP), 'UWV Controlled Remote Access' (UCRA) MySmartXS van KNP	
Voorwaarden	Werkzaamheden zijn onder de volgende voorwaarden toegestaan: 1) De uitvoerende functionarissen zijn a) gehouden aan een geheimhoudingsverklaring; b) bekend met hun werkzaamheden en O&H-programmatuur. 2) De te gebruiken O&H-programmatuur en werkzaamheden zijn beschreven, de risico's m.b.t. IB&P en continuïteit zijn bekend en de risico's zijn afgehandeld. 3) De functionarissen werken met een persoonsgebonden toegang, zodat we weten wie op welk moment een beheerderstoegang heeft gebruikt. 4) De organisatie weet wie kritieke handelingen heeft uitgevoerd. Indien mogelijk steunen we hiervoor op faciliteiten van UCRA en/of logging. 5) Indien de aard van de werkzaamheden hiertoe aanleiding geeft treft UWV aanvullende maatregelen; 6) Indien tijdelijke toegang wordt verleend via MySmartXS, dan is het GSM-nummer waarop de functionaris zijn challenge ontvangt normaal gesproken niet ingevuld. Dit nummer wordt eenmalig ingevuld en na 12 uur weer uit ABS verwijderd.	xxx IDM1 tm IDM 4
Opmerking	De werkzaamheden zijn vrijwel vergelijkbaar met de door eigen medewerkers uitgevoerde NFW. Het verschil is de toegang via UCRA en MySmartXS, dit om meer controle op de werkzaamheden te kunnen houden.	

OTAP-G03	**Uitvoeren van ketentesten t.b.v. go live**	**Richtlijn**
Doel	Het kan in heel bijzondere omstandigheden nodig zijn om een applicatie in de "A"-omgeving te koppelen met een systeem in de "P"-omgeving.	
Geldigheid	P-regime (P en A omgevingen)	
Wie	Door UWV aangewezen functionarissen. Alleen daartoe aangewezen en opgeleide medewerkers van UWV, hosting provider en/of applicatiebouwer mogen deze werkzaamheden uitvoeren. Gezien de potentiële impact van deze actie is het advies van de betrokken security functie van de betrokken divisie(s) en het akkoord van de directie noodzakelijk.	
O&H-programmatuur	*Wordt per situatie beoordeeld.* De systeemeigenaar, projectleider en beherende partij binnen UWV spreken de te gebruiken programmatuur af. Hierbij heeft hergebruik van standaardfaciliteiten de voorkeur.	

Voorwaarden	Werkzaamheden zijn onder de volgende voorwaarden toegestaan: 1) Vooraf is vastgesteld dat UWV geen haalbaar alternatief heeft: a) De test en de koppeling dient een bedrijfsdoel; b) Het realiseren van een testfaciliteit in A is onredelijk duur of levert onvoldoende zekerheid op. 2) De test is zo opgezet dat vervuiling of waarneming van gegevens voorkomen wordt: a) Gebruikte testgegevens kunnen weer uit de systemen worden verwijderd; b) Voorkomen wordt dat met deze koppeling productiegegevens worden waargenomen en/of verwerkt. 3) De uitvoerende functionarissen zijn a) gehouden aan een geheimhoudingsverklaring; b) bekend met hun werkzaamheden en O&H-programmatuur. 4) De gebruikte O&H-programmatuur en werkzaamheden zijn beschreven, de risico's m.b.t. IB&P en stabiliteit & continuïteit zijn bekend en afgedekt. a) De security functie van alle betrokken divisies zijn geraadpleegd bij het beoordelen van deze koppeling; b) Eén of meerdere directeuren heeft de koppeling goedgekeurd. 5) De functionarissen werken met een persoonsgebonden toegang, zodat we weten wie op welk moment een beheerderstoegang heeft gebruikt. 6) De organisatie weet wie kritieke handelingen heeft uitgevoerd: a) De systeemeigenaar wijst kritieke handelingen aan. Dit zijn bijvoorbeeld aanpassen van stamtabellen, het muteren van betaalbestanden of het inzien van beveiligingsinstellingen; b) In Traceerbaarheid wordt voorzien door de inlog, in combinatie met een logboek van de kritieke handelingen en vastlegging van mutatie van gegevens. 7) Gebruikte testdata wordt meteen aantoonbaar vernietigd na de test volgens opgesteld protocol;.	xxx IDM1 tm IDM 4

Bijlage sjabloon gebruik gegevens

Gebruik van gegevenssets met persoonsgegevens in andere omgevingen

Het gebruik van "live" data in de acceptatieomgeving is in principe niet toegestaan. In testomgevingen (Ontwikkel- en testomgeving) is gebruik van "live"data met persoonsgegevens verboden.
Indien maatregelen zijn getroffen is beperkt gebruik van "live" data in de acceptatie-omgeving toegestaan. Uitgangspunt hierin is dat de Acceptatieomgeving onder het P-regime valt (gelijkwaardig aan P-omgeving). Hieronder volgen de stappen van maatregelen voor gebruik van data in andere omgevingen.

Betreft onderwerp / data / proces:

KEUZE aangeven in keuzevak en explain invullen

toepassen van		**keuze** JA	NEE	Toelichting	vervolgstap	**Reden /explain**	
stap 1	Anonimiseren	keuze		Indien data geheel geanonimiseerd is en herleiding naar personen niet mogelijk is, dan is gebruik in acceptatie- of de testomgeving toegestaan	Bij anonimiseren van gegevens in de context van de AVG, zijn in principe geen extra maatregelen nodig, want er zijn geen persoonsgegevens in gebruik. Restrisico bepalen t.b.v. toepassen vervolgstappen.	Reden van niet anonimiseren:	
				Indien data niet geheel is geanonimiseerd of herleiding naar personen is met sleutel of referentiebestand mogelijk (dus eigenlijk gepseudonimiseerd), dan is gebruik in acceptatieomgeving of in geval van noodzaak in de testomgeving met andere / meerdere maatregelen noodzakelijk (zie vervolgstappen)			
stap 2	dataminimalisatie	keuze		Indien data niet is geanonimiseerd, dient zoveel mogelijk dataminimalisatie plaats te vinden. Dataminimalisatie kan plaatsvinden op inhoud (minder velden), op tijd (minder lang beschikbaar) of op doelgroep (beperking van toegang per deel-set van data), bijv. maskeren van data. Daarnaast zijn vervolgens meerdere / andere maatregelen noodzakelijk (zie vervolgstappen)	bepaal welke vervolgstappen doorgevoerd kunnen worden om bij classificatie van gegevens en mate van afbreukrisco passende maatregelen te treffen die een passend beveiligingsniveau garanderen om restrisico geminimaliseerd te hebben; pas naast de mogelijkheden van stappen 2 t/m 4 minimaal toe: *beperking van autorisatie, *uitgebreide logging van handelingen *verwijdering van gebruikte data meteen na gebruik	Reden van niet / gedeeltelijk minimaliseren data:	
				Indien dataminimalisatie niet mogelijk is dienen andere stappen van maatregelen te worden doorlopen			
stap 3	pseudonimiseren	keuze		Indien data is gepseudonimiseerd en herleiding naar personen is niet mogelijk of herleiding naar personen is met sleutel of referentiebestand vrij lastig mogelijk, dan is gebruik in acceptatieomgeving onder een p-regime of in geval van noodzaak in de testomgeving met andere / meerdere maatregelen (zie vervolgstappen) toegestaan		Reden van niet / gedeeltelijk pseudonimiseren data:	
				Indien pseudonimisering niet mogelijk is of herleidbaarheid naar personen is vrij makkelijk, dienen andere stappen van maatregelen te worden doorlopen, waaronder ook een combinatie met real-time monitoring op data leakage door bijv. het USOC.			
stap 4	encryptie	keuze		Indien data is encrypted o.b.v. current best practices en beheerprocedures voor sleutelmanagement toereikend zijn en gedocumenteerd ingericht met en andere / meerdere maatregelen zijn toegepast (zie vervolgstappen), is gebruik in acceptatie onder een p-regime toegestaan		Reden van niet / gedeeltelijk encrypten data:	
				Indien encryptie niet mogelijk is, dienen andere stappen van maatregelen te worden doorlopen			

stap 5	access control	keuze		Indien toegang tot de data met persoonsgegevens beperkt is tot een selecte groep gebruikers, logging en monitoring van gebruik plaatsvindt en data na gebruik wordt verwijderd, is gebruik in acceptatieomgeving onder een p-regime toegestaan (zie vervolgstappen met maatregelen)	beperking van toegangsrechten, logging en eventueel monitoring op gebruik en het zo spoedig mogelijk verwijderen van de gebruikte data met persoonsgegevens is randvoorwaardelijk voor gebruik van persoonsgegevens in de acceptatieomgeving of in geval van noodzaak in de test-omgeving.	Reden van niet / gedeeltelijk beperken autorisatie en bevoegdheden:	
				Indien toegang tot de data met persoonsgegevens niet te beperken is tot een selecte groep gebruikers is expliciete logging van elke handeling noodzakelijk waardoor gebruik in acceptatieomgeving onder een p-regime is toegestaan met andere / meerdere maatregelen (zie vervolgstappen)			
Stap 6	Logging & monitoring	keuze		Indien "live"data met persoonsgegevens wordt gebruikt in de acceptatie-omgeving onder een p-regime, dienen alle handelingen te kunnen worden gelogd en eventueel realtime gemonitord (door wie, wanneer, wat)		Reden van niet / gedeeltelijk loggen en monitoren:	
				Indien geen logging mogelijk is, is gebruik van data met persoonsgegevens niet toegestaan.			
stap 7	verwijderen	keuze		Indien data met persoonsgegevens is gebruikt, dient deze data zo spoedig mogelijk aantoonbaar te worden verwijderd		Reden van niet / gedeeltelijk verwijderen:	
					De reden voor afwijking op het in principe geen gebruik van "live" data met persoonsgegevens in acceptatie- of testomgeving dient opgenomen te worden in het afwijkingen register.		Opgenomen in risicoregister: ja / nee
					De reden voor afwijking op het in principe geen gebruik van "live" data met persoonsgegevens in acceptatie- of testomgeving dient afgestemd te zijn met de leverancier.		Afspraak met leverancier opgesteld met sjabloon ja/nee
	Ondertekening			akkoord BSO	Akkoord Directeur / CIO		Afhankelijk van het restrisico dient ondertekening van dit formulier voor akkoord te geschieden door de BSO en eventueel CISO of de Directeur/CIO in samenspraak met de BSO en de CISO.
				akkoord CISO (indien noodzakelijk)			