OVK Bijlage 1a
Strategisch Beleidskader Beveiliging en Privacy

Uitnodiging tot Inschrijving
EA Vaste en Mobiele Telefonie
>
(TN>)

Bestuurszaken

Strategisch Beleid

Informatiebeveiliging en Privacy (IB&P)

2018-2020

Versie 2.02

Opdrachtgever: Marco van Kampen
Functie: Directeur Bestuurszaken

Auteurs: Stef Schinagl (IB&P Bestuurszaken)
Joseline van Tessel (Juridische Zaken)

Status: Dit document is in compliance met de AVG
Datum: 18 juni 2018

Inhoudsopgave

Documentbeheer

Versie	Datum	Verschil met voorgaande versie	Distributie
0.1	22-07-2013	Eerste concept Beleid 2014-2017.	Coördinatoren B&P
0.2	08-11-2013	Commentaar verwerkt van Coördinatoren.	Coördinatoren B&P, Hoofd BZ Concern, CISO
0.4	22-11-2013	Commentaar verwerkt.	Strategisch B&P Overleg
0.5	10-01-2014	Commentaar verwerkt van Accountants-dienst, CIP en JZ. Toevoeging over digitalise-ring, AVG. Nieuw uitgangspunt.	Directeur BZ en Hoofd BZ Concern
0.6	11-02-2014	Commentaar verwerkt.	Strategisch B&P Overleg
1.0	11-03-2014	Vastgesteld door Groepsraad.	Groepsraad
1.10	06-04-2015	Nieuw Beleidskader IB&P UWV, 2015-2018.	Directeur BZ, CISO, Co-ordinatoren B&P
1.21	30-04-2015	Commentaar verwerkt.	Coördinatoren B&P
1.50	15-10-2015	Risicogestuurd beveiligen toegevoegd.	Projectteam IB&P BZ
1.90	15-12-2015	Commentaar verwerkt, versie 2016-2018.	Coördinatoren B&P
2.00	09-02-2016	Commentaar verwerkt.	
2.01	06-04-2018	Wijzigingsvoorstel AVG van Juridische Zaken	
2.02	14-06-2018	Actualisering in overleg met Juridische Zaken	Intranetversie

1. Doelstelling

UWV vervult een belangrijke maatschappelijke en economische functie in onze samenleving. Als bewaarder en behandelaar verzamelen, verwerken en versturen wij een grote diversiteit en complexiteit aan gevoelige informatie. Het is onze plicht die informatie goed te beveiligen en de privacy van onze klanten te respecteren. Daarnaast kennen wij andere belangrijke drijfveren om het algehele niveau van informatiebeveiliging en 'cyberweerbaarheid' te verhogen en te borgen, zoals:

- De UWV-dienstverlening zal zoveel mogelijk digitaal moeten gaan plaatsvinden;
- UWV participeert in de e-dienstverlening van een compactere rijksoverheid;
- UWV moet voldoen aan steeds strengere wet- en regelgeving ten aanzien van informatiebeveiliging en privacy (compliance eisen);
- UWV zal in toenemende mate worden geconfronteerd met verschillende vormen van cybercriminaliteit en cyberfraude;
- Er is een toenemende noodzaak tot beveiligingsbewustwording van medewerkers, onder andere als gevolg van meer plaatsonafhankelijk werken.

Om de zorgvuldigheid en eenduidige beheersing van onze kritieke gegevensbronnen op een rijksbrede en methodische wijze te effectueren hanteert UWV op tactisch niveau het 'Tactisch IB&P Beleid UWV'.

Dit 'Tactisch IB&P Beleid UWV' bevordert het creëren van een op veiligheid gerichte cultuur, het treffen van de juiste beveiligingsmaatregelen en het inrichten van toezicht op de effectiviteit van de getroffen maatregelen.

Het Beleid wordt voor belangrijke speerpunten verder uitgewerkt in richtlijnen, die onder de verantwoordelijkheid van de beleidskolommen 'Gebouwen', 'Gegevens', 'Medewerkers' en 'ICT' worden opgesteld en uitgerold.

1.1. Evaluatie en bijstelling

Dit document wordt jaarlijks of bij majeure wijzigingen in de omstandigheden geëvalueerd en indien nodig bijgesteld. Het bijgestelde IB&P-beleid wordt vastgesteld namens de Raad van Bestuur en gepubliceerd.

De eerstvolgende evaluatie zal plaatsvinden in het derde kwartaal van 2019.

2. Waarom een Strategisch IB&P Beleid?

2.1. Visie op IB&P

UWV moet aantoonbaar maken dat de aan haar toevertrouwde vertrouwelijke gegevens altijd vertrouwelijk blijven, op een zorgvuldige wijze worden beschermd tegen onbevoegde toegang, verwerking, verstrekking of ontvreemding, en beschikbaar zijn op het moment dat deze nodig zijn.

De maatschappij moet er vanuit kunnen gaan dat alle bij UWV aanwezige gegevens conform de vereisten voor vertrouwelijkheid, integriteit en beschikbaarheid en in overeenstemming met daarvoor geldende wet- en regelgeving op een voor de betrokkene transparante wijze worden gebruikt, beheerd en beschermd.

2.2. Privacy

Om haar taken goed uit te kunnen voeren heeft UWV veel privacygevoelige gegevens van haar klanten nodig. Hier moet UWV zelf zorgvuldig en op een transparante wijze mee omgaan. Dit wordt ook door wettelijke bepalingen vereist. Voor de privacybescherming zijn vooral de Algemene Verordening Gegegevensbescherming (AVG), de Wet SUWI, de wetgeving over medische gegevens, de Archiefwet en de Wet algemene bepalingen burgerservicenummer (Wabb) van belang.

2.3. Digitalisering

UWV ontwikkelt de informatiehuishouding dusdanig dat de UWV-dienstverlening steeds meer digitaal kan plaatsvinden. De overheid en de maatschappij stellen daarbij aan UWV steeds hogere eisen voor digitale veiligheid en privacybescherming, zoals via wetgeving rondom datalekken, meer nadruk op risico-gestuurd beveiligen en de verplichte Privacy Impact Assessments (PIA's)[1].

Verdergaande digitalisering gaat gepaard met bedrijfseconomische voordelen maar ook met meer risico's. De kans op frauduleus handelen of oneigenlijk gebruik neemt toe, omdat digitale gegevens gemakkelijker en breder toegankelijk zijn dan gegevens op papier. Zo kan bijvoorbeeld door onzorgvuldig handelen of hacken vertrouwelijke informatie van de klant in verkeerde handen terecht komen of op een onbevoegde wijze worden veranderd. Daarom is toenemende aandacht nodig voor het borgen van de integriteit van de gegevens en, op diverse plaatsen binnen de UWV werkprocessen, het borgen van de onweerlegbaarheid van bepaalde vitale handelingen op en verwerkingen van digitale gegevens.

Gezien de maatschappelijk taak van UWV is van oudsher de beschikbaarheid en betrouwbaarheid van de informatie belangrijk. Beschikkingen moeten tijdig worden afgegeven, uitkeringen moeten tijdig worden overgemaakt met het juiste bedrag naar het juiste rekeningnummer etc. Dit vereist het borgen van de continuïteit van de webportals van UWV, de informatiesystemen en de infrastructuur.

[1] In de AVG wordt gesproken over de gegevensbeschermingseffectbeoordeling (GEB). In dit beleid wordt hiervoor de overeenkomstige term PIA gebruikt.

Verdergaande digitalisering biedt ook nieuwe mogelijkheden om de kwaliteit van de maatregelen voor Informatie Beveiliging en Privacybescherming (IB&P) op een hoger niveau te tillen. Onder andere door eenmalige opslag en moderne technische beveiligingsfaciliteiten kunnen de vertrouwelijkheid en integriteit van de gegevens nog beter worden gegarandeerd.

2.4. Informatiebeveiliging en privacybescherming (IB&P)

Cybercriminelen zitten niet stil. Zoals onder andere gesignaleerd door het National Cyber Security Center (NCSC) neemt het aantal bedreigende actoren en de daadwerkelijke aanvallen vanuit het cyberdomein in een snel tempo toe. Dit vereist een proactieve opstelling van UWV, zowel bij het voorkomen van cyberaanvallen op haar systemen en gegevens, als het snel en adequaat reageren indien zo een dreiging manifest wordt. Onze 'cyberweerbaarheid' moet voortdurend worden verhoogd.

De maatschappij wordt steeds kritischer over de bescherming van de privacy en het voorkomen van nodeloze inbreuken, waardoor nieuwe beleidsvoorstellen snel leiden tot maatschappelijke discussies over privacyvraagstukken. De wet- en regelgeving rondom dit onderwerp wordt voortdurend aangescherpt, wat steeds leidt tot het verhogen van de eisen voor transparantie en het risico-gestuurd treffen van nieuwe maatregelen.

De combinatie van deze factoren noopt tot een sterke focus op informatiebeveiliging en privacybescherming binnen de dienstverlening van UWV.

3. Hoe zorgt UWV voor adequate bescherming?

UWV besteedt veel aandacht aan het stelsel van maatregelen voor IB&P. Deze maatregelen moeten continu in de pas blijven lopen met de steeds strenger wordende Nederlandse en Europese wet- en regelgeving, en in de pas blijven lopen met de toenemende (cyber) bedreigingen.

3.1. UWV heeft een goede beveiligingsorganisatie

IB&P is een integrale managementverantwoordelijkheid binnen de lijn en beleidsafdelingen. Om op een aantoonbaar zorgvuldige wijze met gegevens om te gaan treft UWV op een risicogestuurde wijze IB&P-maatregelen binnen alle ontwikkelingen en op alle lagen van de organisatie.

De directeur is de eerstverantwoordelijke voor het implementeren van IB&P-maatregelen binnen zijn of haar organisatieonderdeel. De beveiligingsorganisatie ondersteunt de directeur hierin en coördineert de acties die het organisatieonderdeel overstijgen.

Door de toename in het digitaliseren en het intensiveren van de ketenrelaties ontstaan voortdurend nieuwe risico's. Lijnmanagers hebben niet altijd een volledig inzicht in de (cyber) dreigingen, de kwetsbaarheden en de daaruit voortvloeiende risico's. De beveiligingsorganisatie ondersteunt de lijnmanager hierin.

De taken moeten concern breed op elkaar worden afgestemd, wat een effectieve structuur voor IB&P Governance vereist. Hiervoor is de Coalitie IB&P ingericht onder verantwoordelijkheid van de Directeur Bestuurszaken.

3.2. UWV heeft een goede baseline voor IB&P

UWV streeft naar een doorlopende verbetering van de maatregelen voor IB&P. Dit is een randvoorwaarde om de voortschrijdende digitalisering en e-dienstverlening op een veilige

manier te kunnen uitvoeren. Vanuit deze context heeft de Raad van Bestuur van UWV besloten te voldoen aan de vereisten vanuit de 'Baseline Informatiebeveiliging Rijksdienst' (BIR) en zo aan te sluiten bij de wereld van open en breed geaccepteerde standaarden.

UWV heeft een 'Tactisch Beleid IB&P UWV' opgesteld, dat is gebaseerd op internationale best practices en vigerende Nederlandse en Europese wet- en regelgeving. Dit tactisch kader bestaat uit drie secties, namelijk:

- **Sectie A: 'Wettelijk kader IB&P'**
  - Sectie A bevat de IB&P-normen opgelegd vanuit de Wet SUWI, Algemene Verordening Gegevensbescherming (AVG), Wet op de geneeskundige behandelingsovereenkomst (Wgbo), Wet op de beroepen in de individuele gezondheidszorg (Big), Archiefwet, Wet algemene bepalingen burgerservicenummer (Wabb) etc.

- **Sectie B: 'BIR UWV'**
  - Sectie B bevat de normen voor IB&P vanuit de internationale standaard ISO 27001 'Information Security Management System (ISMS)', aangevuld met de door het Ministerie van BZK geformuleerde Rijksmaatregelen die passen bij de bedrijfsprocessen van UWV en specifieke UWV-maatregelen.

- **Sectie C: 'Borging van de BIR Beheersing'**
  - Sectie C beschrijft de Taken, Verantwoordelijkheden en Bevoegdheden van de betrokken organisatieonderdelen en de beleidskolommen 'Gebouwen', 'Gegevens', 'Medewerkers' en 'ICT' binnen UWV.

Het Strategisch en Tactisch Beleid beschrijven de uitgangspunten, doelstellingen en maatregelen voor de technische en organisatorische inrichting van IB&P. Deze worden voor belangrijke speerpunten verder uitgewerkt in richtlijnen, die onder de verantwoordelijkheid van de beleidskolommen worden opgesteld en uitgerold.

3.3. UWV stimuleert beveiligingsbewustwording

Beveiligingsmaatregelen zijn een samenspel tussen technische, fysieke en organisatorische maatregelen. Om de werkprocessen voor de medewerkers werkbaar te houden kan en wil UWV niet alles technisch en fysiek afdichten. Hierom heeft UWV er voor gekozen bewustwording over IB&P te stimuleren bij de medewerkers. Het doel is te bewerkstelligen dat de medewerkers zorgvuldig en bewust omgaan met vertrouwelijke informatie en zich niet om de tuin laten leiden door spam, phishing mails, nep telefoongesprekken, gevaarlijke websites etc.

Digitale ontwikkelingen, zoals e-werken, bring-your-own-device en werken buiten het UWV-kantoor zijn aanknopingspunten voor bewustwordingsprogramma's. Deze programma's helpen medewerkers om op een zorgvuldige en veilige manier gebruik te maken van de moderne technische faciliteiten van UWV.

3.4. UWV stimuleert samenwerking bij beveiliging

Het leervermogen van UWV op het gebied van IB&P is vergroot door het aangaan van samenwerkingsverbanden binnen de overheid en met leveranciers, onder andere via het Centrum Informatiebeveiliging en Privacy (CIP). Op deze wijze worden overheidsmiddelen optimaal gebruikt, doordat deze met een groot aantal organisaties worden gedeeld.

UWV scherpt de aansturing van leveranciers van ICT-middelen en software aan, onder andere via het opleggen van normen en processen voor Secure Software Development (SSD), Beveiligingsovereenkomsten (BVO's) en Logging en Monitoring (LoMo). Op deze wijze eist UWV van de leveranciers dat zij gedegen beveiligingsmaatregelen treffen.

3.5. UWV zet fysieke maatregelen en techniek in voor beveiliging

UWV besteedt veel aandacht aan de veiligheid en beveiliging van haar medewerkers, zowel via facilitaire middelen als via het veilig gebruik van de ICT-middelen.

UWV investeert in het verhogen van de weerbaarheid en het herstelvermogen tegen verstoringen van digitale middelen door cyberaanvallen, cybercrime, moedwillige beschadigende acties etc. Hiertoe is een Security Operations Center (SOC) ingericht, waar ICT-incidenten worden gedetecteerd, geanalyseerd en afgehandeld, en bij voorkeur worden voorkomen.

UWV zet stevig in op het verder verbeteren van de functiescheiding, het autorisatiebeheer en de fysieke en logische toegangsbeveiliging om ongeautoriseerde of onnodige toegang tot de systemen en gegevens zoveel mogelijk te voorkomen.

UWV ontwikkelt nieuwe methoden voor de classificatie van systemen en gegevens om op een pragmatische en effectieve wijze een selectie van een afdoend stelsel van risico-gestuurde maatregelen te kunnen uitvoeren.

3.6. UWV neemt beveiliging van meet af aan mee bij elke verandering

Beveiliging achteraf inbouwen is moeilijker dan vanaf het begin de juiste maatregelen te treffen. UWV hanteert ‘privacy by design’ en ‘privacy by default’ als strategie voor het ontwikkelen van nieuwe werkprocessen en informatiesystemen en bij majeure wijzigingen in de systemen of gegevensverzamelingen. Hiertoe is bijvoorbeeld Secure Software Development (SSD) ontwikkeld met normen en processen.

3.7. UWV reageert adequaat op incidenten met IB&P

Incidenten met ICT en informatie kunnen niet altijd worden voorkomen. Ieder gemeld of geconstateerd incident wordt geanalyseerd en resulteert, waar nodig, in een herstelactie. Hierbij worden de leerpunten vastgesteld om de maatregelen verder te verbeteren en zo de robuustheid van IB&P te verhogen. Indien blijkt dat er sprake is van een datalek wordt de betreffende procedure voor melding doorlopen.

3.8. UWV treft beveiligingsmaatregelen vanuit een risicoafweging

UWV is en blijft een risicomijdende organisatie. Dit komt onder andere tot uitdrukking in de opzet van het ‘Tactisch IB&P Beleid UWV’, de beveiligingsorganisatie, de inrichting van de IB&P overlegplatformen etc.

De regels voor Corporate Governance leggen op dat management besluiten neemt op basis van een zorgvuldige afweging van de risico’s. Ook wetgeving noemt steeds vaker de noodzaak tot het uitvoeren van risicoanalyses, evenals regelgeving zoals de CBP ‘Richtsnoeren Beveiliging Persoonsgegevens’ en het BIR.

Er zijn Europese richtlijnen die het uitvoeren van een risicoanalyse verplichten, zoals voor E-dienstverlening gericht op vertrouwelijkheidrisico’s. In de Europese Algemene Verordening Gegevensbescherming (AVG) zijn Privacy Impact Assessments (PIA’s) verplicht gesteld.

UWV heeft methoden ontwikkeld voor risicoanalyses en PIA’s. Afhankelijk van de uitkomsten van de analyses worden risico’s door een adequaat stelsel van maatregelen geneutraliseerd of expliciet door een directeur geaccepteerd. Hiervan wordt een centrale registratie bijgehouden.

UWV blijft er voor zorgen dat de continuïteit, kwaliteit en veiligheid is geborgd. Dit betekent dat risico's vroegtijdig worden gedetecteerd en op een vakkundige wijze worden aangepakt.

Colofon

Uitgever	UWV Bestuurszaken
Datum	18 juni 2018
Versie	2.02
Document	UWV BZ IBP Strategisch Beleid