Bijlagen

Leslie Pedro
2064231
Juridische Hogeschool Avans-Fontys
Baanbrekers
Waalwijk, 10 januari 2017

Bijlage 1. Privacybeleid

Werkbedrijf Midden Langstraat

Privacyreglement personeelsregistratie

WML 2004

Inclusief 1ste wijziging d.d. 22.10.08 en inclusief 2de wijziging d.d. 22.01.09

Werkbedrijf Midden Langstraat
Zanddonkweg 14
5144 NX WAALWIJK

Contactpersonen : mr. Conny Kleijssen
mr. Bram Brouwer

PRIVACYREGLEMENT
PERSONEELSREGISTRATIE WML 2004

HET ALGEMEEN BESTUUR VAN WML

Gezien het voorstel van het dagelijks bestuur d.d. 26.01.05

Gelet op de ter zake gegeven instemming van de Ondernemingsraad van WML d.d. 07.12.04
Gelet op de ter zake gegeven instemming van de Commissie voor Georganiseerd Overleg d.d. 19.01.05

Gelet op de Wet bescherming persoonsgegevens;

Overwegende dat het uit zorgvuldigheid naar de werknemers toe wenselijk is om vast te stellen op welke wijze wordt omgegaan met hun persoonsgegevens welke zijn vastgelegd in de personeelsregistratie, waarvan de salarisadministratie onderdeel uitmaakt;

besluit

vast te stellen het volgende

Privacyreglement personeelsregistratie WML 2004

Artikel 1 Begripsbepalingen

a. persoonsgegeven is elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.
b. personeelsregistratie is elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen.
c. verwerking van persoonsgegevens is elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.
d. verantwoordelijke is het dagelijks bestuur van WML vertegenwoordigd door de algemeen directeur van WML.
e. beheerder is degene die verantwoordelijk is voor het goed functioneren van (een deel van) de personeelsregistratie. Hij draagt zorg voor naleving van dit reglement en hij draagt er zorg voor dat de gegevens slechts ter beschikking komen van degenen die daartoe gemachtigd zijn. Hij wordt aangewezen door het Dagelijks bestuur van WML (bijlage 1).
f. gebruikers zijn diegenen binnen WML die het geheel of een gedeelte van de personeelsregistratie in het kader van hun werkzaamheden nodig hebben om persoonsgegevens te verwerken, daartoe gemachtigd door de beheerder.
g. betrokkenen zijn degenen op wie een persoonsgegeven betrekking heeft.
h. derde is ieder, niet zijnde de betrokkene, de verantwoordelijke, de beheerder, de gebruiker of enig persoon die onder rechtstreeks gezag van de verantwoordelijke gemachtigd is om persoonsgegevens te verwerken.

Artikel 2 Doelstelling van de personeelsregistratie

De doelstelling van de registratie is het vastleggen van die persoonsgegevens voor zover WML die nodig heeft voor:

a. de aan haar overgedragen uitvoering van de Wet sociale werkvoorziening, de Wet inschakeling werkzoekenden, het verwerken van persoonsgegevens voor derden op basis van dienstverleningsovereenkomst of contract zoals, de Wet reïntegratie arbeidsgehandicapten en het Besluit instroom- en doorstroombanen en het verwerken van persoonsgegevens als gevolg van werkzaamheden in opdracht van het bestuur. Onder de uitvoering c.q. verwerking wordt in ieder geval verstaan:
   - het verwerken van gegevens ten behoeve van de bij of krachtens de wet voorgeschreven rapportage over de uitvoering van voornoemde regelingen;
   - het verwerken van gegevens van betrokkenen om ten aanzien van hen de doelstellingen te kunnen realiseren zoals deze bij genoemde wetten opgedragen zijn;
b. het voeren van een effectief, efficiënt en sociaal verantwoord personeelsbeleid en –beheer;
c. het voldoen aan overige wettelijke verplichtingen.

Artikel 3 Werkingssfeer

Dit reglement is van toepassing op gegevensverwerking in zowel de geautomatiseerde als de niet geautomatiseerde bestanden waarin de personeelsregistratie van WML is opgenomen.

Artikel 4 Bevoegdheid

1. De verantwoordelijke is bevoegd het beheer over de bestanden op te dragen aan een beheerder. Van deze overdracht is een bijlage 1 ingesloten die een onlosmakelijk deel vormt van dit reglement.
2. De gebruikers worden door de beheerder schriftelijk als gebruikers gemachtigd. Van deze functionarissen wordt een lijst bijgehouden die als bijlage 2 een onlosmakelijk deel vormt van dit reglement. Deze lijst bevat behalve de functienamen van de gebruikers tevens een omschrijving van datgene waartoe zij gemachtigd zijn.
3. De bijlage als genoemd in het eerste lid kan door het dagelijks bestuur van WML gewijzigd worden.
4. De bijlage als genoemd in het tweede lid kan door de algemeen directeur van WML gewijzigd worden.

Artikel 5 Categorieën van betrokkenen

De personeelsregistratie kan persoonsgegevens bevatten van:

a. de ambtenaren in dienst van WML;
b. werknemers, welke werkzaam zijn op basis van een dienstbetrekking in het kader van de Wet sociale werkvoorziening, of zijn gedetacheerd in het kader van de Wet sociale werkvoorziening, of welke moeten worden geïndiceerd in het kader van de Wet sociale werkvoorziening;
c. werknemers welke werkzaam zijn op basis van een dienstbetrekking in het kader van de Wet inschakeling werkzoekenden;
d. personen die ingevolge hoofdstuk 7 van de Wet sociale werkvoorziening een arbeidsovereenkomst hebben gesloten met een reguliere werkgever in het kader van Begeleid werken;
e. personen die ingevolge artikel 5 van de Wet inschakeling werkzoekenden een arbeidsovereenkomst hebben gesloten met een reguliere werkgever in het kader van een werkervaringsplaats;
f. personen die ingevolge de uitvoering van de Wet reïntegratie arbeidsgehandicapten een arbeidsovereenkomst hebben gesloten met een reguliere werkgever;
g. personen die werkzaam zijn op basis van het Besluit in- en doorstroombanen;
h. personen die in het kader van de Wet sociale werkvoorziening op de wachtlijst geplaatst zijn;
i. personen, die in het kader van de Wet inschakeling werkzoekenden aangewezen zijn op een voortraject in het kader van artikel 3 Wiw, waaronder begrepen plaatsingen op Arbeidsdiagnostisch Centrum (ADC);
j. bij WML gedetacheerde werknemers van de Stichting Bevordering Werkgelegenheid Midden Langstraat;

k. stagiaires;
l. voormalige en gedetacheerde werknemers van WML;
m. personen in het kader van een traject sociale activering;
n. uitzendkrachten;
o. vrijwilligers.

Artikel 6 Verkrijging van persoonsgegevens

1. De persoonsgegevens van de hiervoor genoemde betrokkenen worden op een behoorlijke en zorgvuldige wijze voor de in artikel 2 genoemde doeleinden verzameld.
2. De persoonsgegevens kunnen worden verkregen bij betrokkene zelf of op een andere wijze dan van betrokkenen zelf (van derden).
3. In beide gevallen deelt de verantwoordelijke aan betrokkene de doeleinden van de verwerking waarvoor de gegevens zijn bestemd mede, voor het moment van verkrijging van informatie, tenzij betrokkene daarvan reeds op de hoogte is.
4. De verantwoordelijke verstrekt nadere informatie voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan gemaakt wordt, nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen.
5. Het derde lid is niet van toepassing, indien de mededeling van de informatie aan de betrokkene onmogelijk blijkt of een onevenredige inspanning kost. In dat geval legt de verantwoordelijke de herkomst van de gegevens vast.

Artikel 7 Verdere verwerking van persoonsgegevens

1. De persoonsgegevens worden na het verzamelen ervan slechts verder verwerkt op een wijze die behoorlijk is, zorgvuldig is en verenigbaar is met de doeleinden waarvoor ze zijn verkregen.
2. Het verwerken van persoonsgegevens dient, gelet op de doeleinden, toereikend, ter zake dienend en niet bovenmatig te zijn. Bovendien dienen de opgenomen persoonsgegevens juist en nauwkeurig te zijn.
3. De verwerking van persoonsgegevens blijft achterwege voor zover een geheimhoudingsplicht uit hoofde van ambt, beroep of wettelijk voorschrift daaraan in de weg staat.

Artikel 8 Inhoud persoonsgegevens

1. De bestanden zullen in principe per betrokkene niet meer persoonsgegevens bevatten of op andere wijze verkregen zijn dan genoemd in bijlage 3, welke een onlosmakelijk deel vormt van dit reglement.
2. Bijlage 3 kan door de beheerder worden gewijzigd, indien aanpassing of uitbreiding noodzakelijk wordt geacht.

Artikel 9 Verstrekking van persoonsgegevens aan gebruikers ter verwerking

Gegevens uit het registratiesysteem kunnen uitsluitend worden verstrekt aan gebruikers voor zover zij door de beheerder daartoe gemachtigd zijn en zij deze gegevens in verband met een goede uitvoering van hun taak behoeven. Voor de door de beheerder verstrekte machtiging wordt verwezen naar bijlage 4, welke een onlosmakelijk deel vormt van dit reglement.

Artikel 10 Verstrekking van persoonsgegevens aan derden

Persoonsgegevens kunnen slechts aan derden verstrekt worden:

a. indien betrokkene voor de verstrekking zijn ondubbelzinnige schriftelijke toestemming heeft verleend, of;
b. de verstrekking noodzakelijk is voor de uitvoering van een overeenkomst waarbij betrokkene partij is, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst;
c. de gegevensverstrekking noodzakelijk is om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is;

d. de gegevensverstrekking noodzakelijk is ter vrijwaring van vitaal belang van de betrokkene;
e. de gegevensverstrekking noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt, of
f. de gegevensverstrekking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op de bescherming van de persoonlijke levenssfeer, prevaleert.
g. Van alle verzoeken om verstrekking van gegevens aan derden en de besluitvorming daaromtrent, wordt aantekening gehouden in het dossier.

Artikel 11 Inzage

1. Betrokkene heeft het recht zich vrijelijk en met redelijke tussenpozen tot de personeelsconsulent te wenden om inzage te verkrijgen in de persoonsgegevens die over hem zijn of worden verwerkt.
2. Inzage vindt altijd plaats onder begeleiding van de P&O consulent (medewerker personeelsadministratie. Zonodig kan toelichting worden gegeven.
3. Indien betrokkene niet in staat kan worden geacht tot een redelijke waardering van zijn belangen terzake, dan treedt een andere persoon als zijn gemachtigde op, zijnde

- de curator of mentor indien de betrokkene onder curatele staat of ten behoeve van hem het mentorschap is gesteld, of
- de persoonlijk gemachtigde, bijvoorbeeld de partner of een familielid;
- een gemachtigde die een advocaat is of een arts, indien er een gewichtige reden is gelegen in de vrees voor schade aan de lichamelijke of geestelijke gezondheid van een betrokkene;
- een gemachtigde die een advocaat is of een arts, indien er een gewichtige reden is gelegen in de vrees voor schade aan de lichamelijke of geestelijke gezondheid van een betrokkene.

4. Van alle verzoeken om inzage en de besluitvorming daaromtrent wordt aantekening gehouden in het dossier.

Artikel 12 Afschrift

1. Aan het recht tot inzage is gekoppeld het recht op een afschrift uit het dossier
2. Bij toestemming tot inzage kan betrokkene, indien hij dit wenst, kopieën laten maken van de aanwezige stukken. Bij het verstrekken van afschriften wordt op het document aangegeven dat het om een kopie handelt.
3. WML is gerechtigd voor de verstrekking van afschriften boven de 100 bladzijden maximaal de kostprijs in rekening te brengen.
4. Van alle verzoeken om afschriften en de besluitvorming daaromtrent wordt aantekening gehouden in het dossier.

Artikel 13 Uitzonderingen

De toepassing van artikel 6, tweede tot en met zesde lid, artikel 7, eerste lid, en artikel 10, 11 en 12 kan achterwege blijven voor zover dit noodzakelijk is in het belang van:
a. de veiligheid van de staat;
b. de voorkoming, opsporing en vervolging van strafbare feiten;
c. gewichtige economische en financiële belangen van de staat en andere openbare lichamen;
d. het toezicht op de naleving van wettelijke voorschriften die zijn gesteld ten behoeve van de belangen onder b en c, of
e. de bescherming van de betrokkene of van de rechten en vrijheden van anderen.

Artikel 14 Correctie

1. De betrokkene of diens wettelijk vertegenwoordiger kan, na inzage in de hem betreffende persoonsgegevens op grond van artikel 11, het hoofd OPJ verzoeken deze te verbeteren, aan te vullen, te verwijderen, of af te schermen indien deze feitelijk onjuist zijn, voor het doel of de doeleinden van de verwerking onvolledig of niet ter zake dienend zijn, dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt.

2. De procedure voor de uitoefening van het correctierecht als bedoeld in het eerste lid is als volgt:
    a. het indienen van een verzoek tot correctie geschiedt schriftelijk bij het hoofd OPJ met opgave van de aan te brengen wijzigingen al dan niet onder overlegging van de vereiste bewijsstukken;
    b. het hoofd OPJ onderzoekt de juistheid van de gegevens en zorgt voor verdere behandeling van het verzoek;
    c. het hoofd OPJ bericht betrokkene binnen vier weken na ontvangst van het verzoek schriftelijk of dan wel in hoeverre hij daaraan voldoet.
    d. als het hoofd OPJ beslist dat het verzoek tot correctie terecht is, draagt hij er zorg voor dat de beslissing tot verbetering, aanvulling, verwijdering of afscherming binnen vier weken wordt verricht;
    e. indien het hoofd OPJ van mening is, dat er geen aanleiding bestaat de opgenomen persoonsgegevens te corrigeren, deelt hij dit conform het gestelde onder c met redenen omkleed schriftelijk aan betrokkene mede.
3. Binnen zes weken na ontvangst van een schriftelijke mededeling van een weigering als bedoeld in het tweede lid onderdeel e, kan betrokkene een bezwaarschrift indienen bij het dagelijks bestuur van WML.

Artikel 15 Geheimhoudingsplicht persoonsgegevens en beveiliging

1. Een ieder die de beschikking krijgt over persoonsgegevens waarvan hij het vertrouwelijk karakter kent of redelijkerwijs moet vermoeden en voor wie niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift ter zake van die gegevens een geheimhoudingsplicht geldt, behoudens afwijkende verplichtingen, is verplicht tot geheimhouding daarvan, behoudens voor zover enig wettelijk voorschrift hem tot bekendmaking verplicht.
2. De beheerder, systeembeheerder en applicatiebeheerder dragen de zorg voor het aanleggen van passende en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligings-niveau gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen.
3. Een gelijke plicht zoals genoemd in lid 2 van dit artikel ligt op de gebruikers ten aanzien van het door hen te gebruiken geheel of gedeelte van de personeelsregistratie.

Artikel 16 Bewaren van persoonsgegevens

1. Persoonsgegevens worden niet langer bewaard in een vorm die het mogelijk maakt de betrokkene te identificeren, dan noodzakelijk is voor de verwerkelijking van de doeleinden waarvoor zij worden verzameld en vervolgens verder worden verwerkt, zie bijlage 6 van dit reglement**.**
2. In sommige gevallen is het toegestaan gegevens langer te bewaren dan de (minimale) termijnen genoemd in bijlage 6 van dit reglement, namelijk wanneer dit noodzakelijk is ter voldoening aan een wettelijke bewaarplicht. De Archiefwet voorziet in een bewaarplicht voor archiefbescheiden van de overheid. De in bijlage 6 genoemde (minimum) termijnen gaan boven de in het Vrijstellingsbesluit WBP genoemde termijnen.
3. Betrokkene heeft recht op vernietiging van (delen van) het dossier. Zo'n verzoek kan worden geweigerd indien de gegevens vallen onder een wettelijke bewaarplicht of indien bewaring van de gegevens een aanmerkelijk belang is voor de beheerder.
4. Verzoek tot vernietiging van (delen van) het dossier geschiedt volgens dezelfde procedure als genoemd in artikel 14 lid 2 (procedure uitoefenen van het correctierecht).
5. Vernietiging op verzoek van betrokkene komt voor diens risico. In voorkomende gevallen dient aantekening te worden gemaakt dat het dossier of delen van het dossier zijn vernietigd op verzoek van betrokkene.

Artikel 17 Gebruik persoonsgegevens voor onderzoek en statistiek

1. Onder bepaalde voorwaarden mogen persoonsgegevens langer bewaard worden dan bepaald in artikel 16, voorzover ze voor historische, statistische of wetenschappelijke doeleinden worden bewaard en de verantwoordelijke de nodige voorziening heeft getroffen ten einde te verzekeren dat de desbetreffende gegevens uitsluitend voor deze specifieke doeleinden worden gebruikt.
2. Betrokkene moet van tevoren in algemene zin bekend zijn gemaakt dat zijn gegevens gebruikt kunnen worden voor onderzoek en statistiek en hij heeft hiertegen geen uitdrukkelijk bezwaar gemaakt.

Artikel 17a Klachtbehandeling
Betrokkene kan een klacht indienen op grond van de "Verordening op de behandeling van klachten WML 2003", indien er bij betrokkene sprake is van ongenoegen over de wijze waarop een bestuursorgaan of een medewerker van WML zich in een bepaalde aangelegenheid in het kader van dit reglement jegens betrokkene heeft gedragen.

Artikel 18 Huishoudelijk reglement
Naar aanleiding van dit privacyreglement is een huishoudelijk reglement opgesteld, opgenomen in bijlage 5, welke deel uitmaakt van dit reglement, waarin een meer concrete invulling wordt gegeven aan de manier waarop gebruikers van persoonsgegevens dienen om te gaan met de hen ter beschikking staande persoonsgegevens.

Artikel 19 Hardheidsclausule
1. Alle overige registraties, niet zijnde personeelsregistraties, zijn, voorzover mogelijk, onderhevig aan hetgeen is bepaald in dit reglement inclusief bijlagen.
2. In gevallen waarin dit reglement en/of de bijlagen niet voorzien, wordt beslist door de algemeen directeur van WML.

Artikel 20 Benaming
Dit reglement kan worden aangehaald als "Privacyreglement personeelsregistratie WML 2004"

Artikel 21 Bekendmaking
Bekendmaking van de vaststelling van dit reglement geschiedt door het opnemen van dit reglement inclusief bijlagen in het handboek OPJ en in B-wise (intranet).

Artikel 22 Intrekking
Het Privacyreglement personeelsregistratie WML datum januari 2003 wordt met de inwerkingtreding van het Privacyreglement personeelsregistratie WML 2004 ingetrokken.

Artikel 23 Inwerkingtreding
Dit reglement treedt in werking op datum vaststelling van dit reglement door het Algemeen Bestuur.

Aldus vastgesteld in de openbare vergadering van het algemeen bestuur van 2 februari 2005, nadien gewijzigd d.d. 22 oktober 2008 (1e wijziging) en 22-01-'09 2e wijziging..

Toelichting op het privacyreglement personeelsregistratie WML

Artikel 1 Begripsbepalingen

Persoonsgegevens: Alle gegevens die informatie kunnen verschaffen over een identificeerbare natuurlijke persoon moeten als persoonsgegevens worden beschouwd. De definitie bevat een aantal elementen dat expliciet aandacht vraagt.

1. het moet gaan om informatie 'betreffende' een natuurlijke persoon;
2. deze persoon moet zijn geïdentificeerd of althans identificeerbaar zijn.

Als er aan één van beide elementen niet is voldaan, dan is er geen sprake van persoonsgegevens en is de wet niet van toepassing.

Gegevens die betrekking hebben op een persoon

Het is relevant of de gegevens informatie over een persoon bevatten. In veel gevallen, zoals bij feitelijke of waarderende gegevens over eigenschappen, opvattingen of gedragingen, zal dit uit de aard van de gegevens voortvloeien. In andere gevallen zal mede aandacht moeten worden besteed aan de context waarin het gegeven wordt vastgelegd en gebruikt.

Als gegevens mede bepalend zijn voor de wijze waarop de betrokken persoon in het maatschappelijk verkeer wordt beoordeeld en behandeld, moeten die gegevens als persoonsgegevens worden aangemerkt. Het (maatschappelijk) gebruik dat van gegevens wordt gemaakt is dus medebepalend voor de beantwoording van de vraag of sprake is van een persoonsgegeven.

Gegevens die een neerslag vormen van een over een bepaalde persoon genomen beslissing, kunnen worden beschouwd als een deze persoon betreffend persoonsgegeven. Ook gegevens die niet direct betrekking hebben op een bepaalde persoon kunnen soms over een bepaalde persoon informatie verschaffen, bijvoorbeeld wanneer de arbeidsproductiviteit van een werknemer gemakkelijk in kaart kan worden gebracht. Tevens dienen telefoonnummers, kentekens van auto's en postcodes met huisnummers onder omstandigheden als een persoonsgegeven te worden aangemerkt.

Gegevens die naar hun aard niet op personen betrekking hebben noch – gezien de context waarin zij worden verwerkt – mede bepalend zijn voor de wijze waarop een persoon in het maatschappelijk verkeer wordt beoordeeld of behandeld, zijn geen persoonsgegevens. In zo'n geval gaat het om zuivere objectgegevens.

Gegevens die betrekking hebben op overledenen of rechtspersonen, zijn geen persoonsgegevens als bedoeld in dit artikel.

De identificeerbaarheid van een persoon

Uitgangspunt is dat een persoon identificeerbaar is indien zijn identiteit redelijkerwijs, zonder onevenredige inspanning, vastgesteld kan worden.

Twee factoren spelen hierbij een rol: de aard van de gegevens en de mogelijkheden van de verantwoordelijke om de identificatie tot stand te brengen.

a. De aard van de gegevens

Een persoon is identificeerbaar indien sprake is van gegevens die alleen of in combinatie met andere gegevens, zo kenmerkend zijn voor een bepaalde persoon dat deze aan de hand daarvan kan worden geïdentificeerd.

Van *direct identificerende gegevens* is sprake wanneer gegevens betrekking hebben op een persoon waarvan de identiteit zonder veel omwegen eenduidig vast te stellen is. Direct identificerende gegevens zijn gegevens als naam, adres, geboortedatum, die in combinatie met elkaar dermate uniek

en dus kenmerkend zijn voor een bepaalde persoon dat deze in brede kring met zekerheid of met een grote mate van waarschijnlijkheid, kan worden geïdentificeerd.

Van *indirect identificeerde gegevens* is sprake wanneer de gegevens niet direct tot identificatie van een bepaald persoon leiden maar via nadere stappen de gegevens in verband kunnen worden gebracht met een bepaalde persoon. De gegevens kunnen zijn ontdaan van de naam, doch onder omstandigheden door combinatie met andere gegevens weer worden teruggebracht tot een bepaalde persoon.

Daarnaast zijn er gegevens die zodanig uniek zijn dat zij ook identificerend zijn, zoals het sofinummer of unieke biometrische gegevens zoals stem, vingerafdruk of DNA-profiel.

Het verwijderen van direct identificerende kenmerken biedt op zichzelf niet altijd voldoende garantie dat geen sprake meer is van persoonsgegevens. Door middel van spontane herkenning, vergelijking van gegevens en/of koppeling aan gegevens uit andere bron, kan immers desondanks, soms zonder bijzondere inspanning, identificatie tot stand worden gebracht. Is echter het risico van spontane herkenning redelijkerwijs uitgesloten, dan kan worden aangenomen dat er géén sprake is van persoonsgegevens.

b. De mogelijkheden van de verantwoordelijke om identificatie tot stand te brengen
Gekeken moet worden naar alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs door de verantwoordelijke dan wel enig ander persoon zijn in te zetten om die persoon te identificeren. Uitgegaan moet worden van een redelijk toegeruste verantwoordelijke. In concrete gevallen moet echter wel rekening gehouden worden met bijzondere expertise, technische faciliteiten en dergelijke van de verantwoordelijke.

Een gegeven is géén persoonsgegeven indien doeltreffende maatregelen zijn getroffen waardoor een werkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten.

Bestand: Een bestand kan zowel geautomatiseerde als niet geautomatiseerde bewerkingen bevatten. Van een bestand is sprake als de persoonsgegevens deel uitmaken van een gestructureerd geheel dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen.

Een (gestructureerd) geheel
De gegevensverwerkingen of de verzameling op grond van meer dan één kenmerk moet(en) een onderlinge samenhang vertonen. Onderlinge samenhang kan blijken uit een gemeenschappelijke bestemming of uit het feit dat de verzameling in de praktijk als een geheel wordt beschouwd.
De samenhang kan zitten in een vooraf aangebrachte structuur van de verzameling of in een raadpleegmethodiek die samenhang brengt in ogenschijnlijk willekeurige gegevensverwerkingen.

Voor de vraag of er sprake is van één of meerdere bestanden is van belang het doel of de doelen van de verwerkingen en het feitelijk gebruik van de gegevens.

Het criterium gestructureerd geheel is eveneens van belang om vast te stellen of er sprake is van één of wellicht meerdere bestanden. Alsdan is niet zozeer de fysieke verschijningsvorm als wel de logische samenhang van de verzameling van belang. Dit brengt met zich dat back-ups en schaduwbestanden niet als een afzonderlijk bestand moeten worden aangemerkt maar zijn te beschouwen als hulpmiddelen bij het voeren van een bestand ten dienste waarvan zij zijn aangelegd.

Systematische toegankelijkheid
Het gaat hierbij vooral om de vraag of verzamelingen een duidelijke, vooraf met het oog op raadpleging aangebrachte structuur bezitten. De methode van gegevensopslag en –verwerking is van belang. De inhoud van het bestand moet met het oog op doeltreffende raadpleging volgens bepaalde criteria zijn aangelegd.

Dossierverzamelingen die uitsluitend bestaan uit en hoeveelheid op alfabet gerangschikte dossiers, met losse aantekeningen en min of meer chronologisch geordende documenten van velerlei aard, zullen niet voldoen aan het vereiste van systematische toegankelijkheid. Tot slot dient het gestructureerd geheel van gegevens betrekking te hebben op verschillende personen.

Verwerking van persoonsgegevens: **Het object van regeling is het verwerken van persoonsgegevens. Het verkrijgen van gegevens is eveneens een vorm van verwerken van gegevens.**

Onder 'elk geheel van handelingen met betrekking tot persoonsgegevens' kan worden verstaan een bundeling van verwerkingshandelingen die in het maatschappelijk verkeer als een eenheid wordt beschouwd. Daarnaast is denkbaar dat dezelfde verwerkingshandelingen met betrekking tot bepaalde persoonsgegevens naar de wettelijke maatstaven als een geheel van verwerkingen moet worden aangeduid.

Onder 'handelingen met betrekking tot persoonsgegevens' dienen alle verwerkingen waaraan persoonsgegevens kunnen worden onderworpen, te worden verstaan.

Zowel geautomatiseerde als niet geautomatiseerde handelingen met betrekking tot persoonsgegevens vallen onder het begrip 'gegevensverwerking' met dien verstande dat ten aanzien van de niet geautomatiseerde verwerkingen het WBP slechts van toepassing is voor zover deze in een bestand zijn opgenomen of bestemd zijn om daarin te worden opgenomen.

Cruciaal blijft dat de verwerking gepaard moet gaan met de mogelijkheid daarop (enige) invloed uit te kunnen oefenen. Niet relevant is of de invloed ook daadwerkelijk wordt uitgeoefend.

Het begrip gegevensverwerking omvat het gehele proces dat een gegeven doormaakt vanaf het moment van verzamelen van een gegeven tot aan het moment van vernietiging. Iedere handeling of geheel van handelingen met betrekking tot het gegeven, al dan niet uitgevoerd met behulp van geautomatiseerde procédés, valt daaronder.

Ook de verwerking van persoonsgegevens voor de uitvoering van bepaalde zoekopdrachten met behulp van daartoe geschreven programma's, al dan niet verricht door de verantwoordelijke zelf, valt onder de algemene normering van gegevensverwerking.

Verantwoordelijke: Het begrip 'verantwoordelijke' knoopt in eerste instantie aan bij de vaststelling van het doel van de verwerking. De vraag is wie uiteindelijk bepaalt of er gegevens worden verwerkt en zo ja, welke verwerking, van welke persoonsgegevens en voor welk doel. Tevens is van belang wie beslist over de middelen voor die verwerking; de vraag op welke wijze de gegevensverwerking zal plaatsvinden.

Bij de beantwoording van de vraag wie de verantwoordelijke is onder de WBP uitgegaan van degene die bevoegd is doel en middelen vast te stellen. Dat laat onverlet dat het feitelijk beheer over de gegevensverwerking aan een ander kan worden gemandateerd. In de meeste gevallen zal deze ander wat betreft het geheel van de gegevensverwerking hiërarchisch ondergeschikt zijn aan de verantwoordelijke.

Uitgangspunt bij de invulling van het begrip 'verantwoordelijke' is de bestaande structuur van het civielrechtelijke en bestuursrechtelijke personen- en organisatierecht. De WBP staat evenwel niet in de weg aan een regeling waarbij in de statuten van de betrokken rechtspersonen of via een overeenkomst aan een bepaalde rechtspersoon binnen het concern de bevoegdheid wordt toegekend om doel en middelen van de gegevensverwerkingen binnen het concern te bepalen. De genoemde rechtspersoon is dan verantwoordelijke, omdat de juridische zeggenschap krachtens de getroffen regeling bij die rechtspersoon berust.

Artikel 2 Doelstelling van de personeelsregistratie

Artikel 7 van de WBP schrijft voor dat persoonsgegevens voor welbepaalde en uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld.
'Welbepaald en uitdrukkelijk omschreven' houdt in dat men geen gegevens mag verzamelen zonder een precieze doelomschrijving. Het doel moet bepaald zijn alvorens men tot verzamelen overgaat.
'*Welbepaald'* houdt in dat de doelomschrijving duidelijk moet zijn, niet zo vaag of ruim dat zij tijdens het verzamelproces geen kader kan bieden waaraan getoetst kan worden of de gegevens nodig zijn voor dat doel of niet. Van gerechtvaardigde doelen kan alleen sprake zijn als deze met inachtneming van artikel 8 WBP kunnen worden bereikt.

In artikel 8 WBP is immers een limitatieve opsomming opgenomen van gronden voor toelaatbare gegevensverwerking.

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

Bij elke verwerking moet voldaan zijn aan de beginselen van *proportionaliteit* en *subsidiariteit*. Het *proportionaliteitsbeginsel* houdt in dat de inbreuk op de belangen van de betrokkene bij de verwerking niet onevenredig mag zijn in verhouding tot het met de verwerking te dienen doel. Ingevolge het *subsidiariteitsbeginsel* mag het doel waarvoor de persoonsgegevens worden verwerkt in redelijkheid niet op een andere, voor de bij de verwerking van persoonsgegevens betrokkene minder nadelige wijze kunnen worden verwerkelijkt.

Artikel 3 Werkingssfeer

Artikel 2 WBP heeft betrekking op iedere geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens alsmede op handmatig gevoerde gegevens, voor zover deze in een bestand voorkomen of bestemd zijn om daarin te worden opgenomen.
Van een geautomatiseerde verwerking is sprake indien gebruik wordt gemaakt van middelen en methoden van geautomatiseerde gegevensverwerking.
Als gevolg van de werking van de WBP is het reglement dan ook van toepassing op zowel de geautomatiseerde als de niet geautomatiseerde bestanden.

Artikel 6 Verkrijging van persoonsgegevens

Artikel 6, eerste lid

Op grond van artikel 1, onderdeel o WBP omvat het *verzamelen van persoonsgegevens* het verkrijgen van persoonsgegevens. Het enkele vragen naar persoonsgegevens valt niet onder het begrip 'verzamelen'. Er is immers nog geen sprake van een 'verkrijging van persoonsgegevens'. Er is pas sprake van verzamelen van persoonsgegevens wanneer één of meer persoonsgegevens daadwerkelijk worden verworven.

Op grond van artikel 6 Wbp is bepaald dat persoonsgegevens in overeenstemming met de wet, *behoorlijk* en *zorgvuldig* moeten worden verwerkt. Voorwaarde voor een behoorlijke en zorgvuldige verwerking van gegevens is dat de betrokkenen van het bestaan van de verwerkingen kennis kunnen hebben en, wanneer van hen gegevens worden verkregen, daadwerkelijk en volledig worden ingelicht over de omstandigheden waaronder deze gegevens worden verkregen. Praktijken waarbij bijvoorbeeld onopgemerkt gegevens omtrent personen worden vergaard en verwerkt, al dan niet met behulp van technische hulpmiddelen, zijn dus ongeoorloofd.

Artikel 6, tweede en derde lid
Er kunnen twee vormen van actieve informatieverkrijging worden onderscheiden. De verkrijging van de gegevens:
1. bij de betrokkene zelf doordat de betrokkene zelf actief zijn persoonsgegevens ter beschikking stelt en
2. op andere wijze.

De artikelen 33 en 34 WBP bepalen dat de verantwoordelijke verplicht is zijn identiteit bekend te maken aan de betrokkene en deze te informeren over de doeleinden van de verwerking, *tenzij de betrokkene daarvan 'reeds op de hoogte is'*. Er wordt hierbij uitgegaan van een ongelijkwaardigheid van partijen.
Onder het regime van de WBP zal de verantwoordelijke zich pas ontslagen mogen achten van zijn informatieplicht, als hij weet dat de betrokkene op de hoogte is. *Er is geen onderzoeksplicht van betrokkene vanwege de vaak ongelijkwaardigheid van partijen.*
Echter, het 'op de hoogte zijn' mag de verantwoordelijke op uiteenlopende wijze, afhankelijk van de omstandigheden, aannemen. Beschikt de betrokkene over de informatie dan is hij daarmee op de hoogte, ongeacht of hij het initiatief heeft genomen de informatie ook tot zijn bewustzijn te brengen. Hoewel de verantwoordelijke dus niet zonder meer ervan mag uitgaan dat de betrokkene in een bepaalde situatie wel kan weten of weet dat, door wie en hoe de gegevens worden verwerkt, kunnen ook bepaalde gedragingen of verklaringen van betrokkene aanleiding geven tot het gerechtvaardigde vermoeden van de verantwoordelijke dat de betrokkene daarvan op de hoogte is. Het gaat om gedragingen of verklaringen die in het maatschappelijk verkeer de betrokkene kunnen worden toegerekend als blijk van het feit dat hij op de hoogte is.

Verkrijging van gegevens bij betrokkene zelf
Worden de gegevens verkregen bij de betrokkene zelf dan dient deze op de hoogte te worden gesteld op het moment van vergaring van gegevens ingevolge artikel 33 WBP. De verplichting van de verantwoordelijke om op eigen initiatief betrokkene op de hoogte te stellen van het bestaan van de gegevensverwerking is een belangrijk instrument om het gegevensverkeer transparant te maken.

De omvang van de informatieverplichting is mede afhankelijk van de wijze waarop het contact tot stand komt. In beginsel zal op de verantwoordelijke een extra verantwoordelijkheid tot informeren rusten als hij zelf het initiatief neemt tot het contact met de betrokkene.

Verkrijging van persoonsgegevens op andere wijze
Artikel 34 WBP regelt de situatie dat de gegevens op een *andere wijze* worden verkregen, dus buiten de betrokkene om, hetzij bij *derden*, hetzij door *eigen observatie*.
In het geval van gegevensvergaring bij een ander dan de betrokkene zal de verantwoordelijke de betrokkene moeten informeren indien de gegevens worden vastgelegd dan wel, indien de verstrekking van de gegevens aan een derde wordt overwogen, *uiterlijk op het moment van eerste verstrekking*. Er vindt in dat geval bij de vergaring geen (direct) contact plaats tussen de betrokkene en de verantwoordelijke. Dit contact zal de verantwoordelijke daarentegen zoeken bij vastlegging respectievelijk eerste verstrekking. Daarbij zal het contact specifieker zijn naarmate het aantal bij de verwerking betrokkenen specifieker bepaalbaar is.

Voor de vraag of het moment van vastlegging dan wel verstrekking aan derden geldt als het moment van informatieverstrekking zijn de objectieve bedoelingen van de verantwoordelijke doorslaggevend. Heeft hij geen oogmerk te verstrekken dan geldt het moment van vastleggen. Hij dient dan de betrokkene zo spoedig als redelijkerwijs mogelijk is van informatie te voorzien. *Heeft de verantwoordelijke daarentegen wel de bedoeling aan derden te verstrekken, dan kan in ieder geval met de verstrekking géén begin worden gemaakt dan nadat de betrokkene is geïnformeerd.*

Artikel 6, vierde lid
Het is steeds nodig dat de *identiteit van de verantwoordelijke* en het *doel van de verwerking* waarvoor de gegevens zijn bestemd, aan de betrokkenen worden meegedeeld. Hij zal de betrokkene nader moeten informeren opdat er sprake is van een gegevensverwerking die als rechtmatig kan worden aangemerkt.

Wanneer informatie wordt gevraagd in het kader van een te sluiten overeenkomst kan het voorkomen, dat informatie van de betrokkene wordt gevraagd, waarvan de beantwoording niet essentieel is voor het sluiten van de overeenkomst. Het geven van een antwoord kan achterwege blijven zonder dat daarmee het gevraagde in gevaar komt. In dergelijke gevallen hoort het tot de eisen van zorgvuldige gegevensverwerking de betrokkene van deze omstandigheden op de hoogte te stellen.

Als aan de *informatieplicht* overeenkomstig de artikelen 33 en 34 WBP is voldaan, zijn deze artikelen uitgewerkt en zal er ook geen sprake meer kunnen zijn van onrechtmatige verkrijging wegens niet nakoming van deze verplichting.

Artikel 6, zesde lid
De plicht om de betrokkene van de gegevenverkrijging in kennis te stellen is echter niet absoluut. Dit blijkt uit hetgeen bepaald is in artikel 34 WBP. Het is niet altijd mogelijk betrokkene te achterhalen. Ook zijn er gevallen waarin het theoretisch mogelijk zou zijn om de betrokkene op de hoogte te stellen, maar waarbij de vereiste inspanning in geen verhouding staat tot het doel dat daarmee gediend wordt. In dat geval moet er echter zijn voorzien in compenserende waarborgen. De verantwoordelijke dient dan vast te leggen van wie en op welke wijze hij de gegevens heeft verkregen.

Artikel 7 Verdere verwerking van persoonsgegevens
Het verdere verwerken van persoonsgegevens dient eveneens te voldoen aan de eisen zoals die in artikel 6 verwoord zijn en uitgewerkt in de toelichting op artikel 6, eerste lid van dit reglement.

Artikel 9, eerste lid WBP bepaalt vervolgens dat de gegevens (vervolgens) niet verder mogen worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen. *Gegevens kunnen dus gebruikt worden voor andere doeleinden dan waarvoor zij verzameld zijn, mits deze doeleinden verenigbaar zijn met het oorspronkelijke doel waarvoor zij worden verwerkt.*

Bij de beantwoording van de vraag of er sprake is van verenigbaar gebruik leggen uiteenlopende factoren gewicht in de schaal. Een aantal factoren is ter nadere invulling van *de verenigbaarheidseis*, in het tweede lid opgesomd. Het gaat nadrukkelijk niet om een limitatieve opsomming. Evenmin kan worden gesteld dat een van de factoren op zichzelf van doorslaggevende betekenis is. Elk van de factoren dienen in onderling verband te worden beoordeeld en gewogen ter beantwoording van de vraag of sprake is van verenigbaar gebruik.

1) De bepaling inzake verenigbaar gebruiken geeft uitdrukking aan het doelbindingsprincipe, daarom eerst bezien welke verwantschap er bestaat tussen de beide doelen;
2) De aard van de betreffende gegevens. Gegevens kunnen gevoelig zijn door de context waarin zij worden gebruikt. Hoe gevoeliger het gegeven, hoe minder snel sprake is van verenigbaar gebruik bij afwijking van het oorspronkelijk doel;
3) In welke mate ondervindt betrokkene de gevolgen van een doelwijziging. Worden de gegevens gebruikt als basis voor mogelijke beslissingen met betrekking tot hem, dan is er eerder sprake van onverenigbaar gebruik dan wanneer de gegevens worden gebruikt voor wetenschappelijk onderzoek of voor de toezending van bepaalde boodschappen.

Eén vorm van gebruik is het koppelen van persoonsgegevens. De algemene regels over het verenigbaar gebruik zijn op gegevensverwerkingen van toepassing die als koppeling worden aangemerkt. De eis van verenigbaar gebruik brengt met zich mee dat persoonsgegevens kunnen worden gekoppeld wanneer ten minste aan de eis is voldaan dat de doeleinden waartoe de gegevens oorspronkelijk zijn verzameld met elkaar verenigbaar zijn. In het algemeen zal gelet op de toepasselijkheid van de eis van verenigbaar gebruik vooral gezocht moeten worden naar zodanige vormen van verwerking dat de mogelijk vast te stellen gegevens niet buiten de kring van personen bekend worden dan ten behoeve van wie de koppeling heeft plaatsgevonden. Dit dient door technische en organisatorische maatregelen te worden voorkomen.

Artikel 7, tweede lid

Het doel waarvoor de gegevens zijn verzameld en vervolgens worden verwerkt, is bepalend voor de hoeveelheid en de soort gegevens die onderwerp van verwerking vormen. De gegevens dienen met het oog op dat doel *toereikend*, *ter zake dienend* en *niet bovenmatig* te zijn (eerste lid). Tevens dienen persoonsgegevens juist en nauwkeurig te zijn (tweede lid). Het artikel legt op degene die de gegevens verwerkt een continue verplichting tot toetsing.

Indien de verantwoordelijke een zo beperkt aantal gegevens verwerkt dat in redelijkheid niet kan worden gezegd dat hij daarmee, gelet op de doeleinden waarvoor hij de gegevens wenst te verwerken, een juist beeld van de betrokkene heeft, overtreedt hij het voorschrift dat de gegevens met het oog op het doel waarvoor ze worden verwerkt, toereikend dienen te zijn. Daar staat tegenover dat de gegevens die worden verwerkt evenmin met het oog op het doel waarvoor ze worden verwerkt bovenmatig mogen zijn. Tot slot dienen de gegevens met het oog op het doeleind waarvoor ze worden verwerkt ter zake dienend te zijn.

Het voorschrift in artikel 11, tweede lid WBP gaat uit van een *inspanningsverplichting voor de verantwoordelijke*: de verantwoordelijke moet de nodige maatregelen treffen opdat de gegevens juist en nauwkeurig zijn. Op hem wordt geen absolute verplichting gelegd. Een garantie voor de juistheid van de gegevens kan niet van hem worden gevergd.
Met ‘nodige maatregelen’ wordt uitgedrukt dat alle maatregelen moeten worden getroffen die in redelijkheid kunnen worden gevergd.

Artikel 10 Verstrekking van persoonsgegevens aan derden

In de WBP is het verstrekken van gegevens aan derden niet meer afzonderlijk als bepaling opgenomen met eisen waaraan de derdenverstrekking dient te voldoen. De derdenverstrekking valt nu immers onder het begrip ‘verwerken van persoonsgegevens’. De eisen die gesteld worden aan het verwerken, waaronder het verzamelen, van persoonsgegevens gelden daarmee ook voor de derdenverstrekking. Om de derdenverstrekking in het privacyreglement personeelsregistratie WML toch aandacht te geven zijn de gronden uit artikel 8 WBP aangegeven, waarop gegevens slechts verwerkt mogen worden. Dit geldt in feite dus voor het gehele proces van het verwerken van gegevens. Zie ook de toelichting onder artikel 2 van het Privacyreglement personeelsregistratie WML.

Artikel 11 Inzage

Op grond van artikel 35 WBP is een belangrijk onderdeel van het *transparantiebeginsel* is dat een ieder in beginsel in de gelegenheid moet zijn om na te kunnen gaan of zijn gegevens worden verwerkt. De betrokkene die de wijze waarop zijn gegevens worden verwerkt onrechtmatig vindt, moet in staat zijn dit zelf in rechte aan te vechten.

De term *‘met redelijke tussenpozen’* zorgt ervoor dat het aan betrokkene niet toegestaan is de verantwoordelijke meer dan gemiddeld en noodzakelijk te benaderen met verzoeken om inzage.

In artikel 35 WBP wordt gesproken over het door de verantwoordelijke doen van een mededeling over het wel of niet verwerken van persoonsgegevens. Hij moet daarvan een volledig overzicht geven, een

omschrijving van de doeleinden voor verwerking en allerlei andere informatie. Voor wat betreft de reikwijdte van het artikel strekt het voor WML te ver. Immers, een werknemer weet al bij indienstneming dat er gegevens over hem verwerkt gaan worden en worden de gegevens ook veelal bij hem zelf opgevraagd. Om de toepassing van dit artikel dan ook meer op de praktijk toe te passen, is ervoor gekozen om géén opgave te doen van de informatie, maar om betrokkene in staat te stellen zijn eigen dossier in te zien. In dit dossier zijn alle persoonsgegevens die verwerkt worden opgenomen. Wat dat betreft gaat WML in dit opzicht zelfs verder dan hetgeen zij bij WBP opgelegd krijgt.

Artikel 13 Uitzonderingen
Het recht op bescherming van de persoonsgegevens kan niet in absolute zin worden geformuleerd. De samenleving kan niet functioneren wanneer niet onder bepaalde omstandigheden op de vastgestelde beginselen een uitzondering kan worden gemaakt.

De gronden om een uitzondering te maken zijn in de bepaling zelf opgenomen. De toepasselijkheid van deze gronden is onderworpen aan het *'noodzakelijkheidscriterium'*.

Artikel 14 Correctie
Bij een verzoek tot correctie hoeft het niet altijd te gaan om een de verantwoordelijke verwijtbare onrechtmatige gedraging. Indien bepaalde persoonsgegevens feitelijk onjuist zijn, heeft de betrokkene ook recht op verbetering zonder dat de verantwoordelijke tekort is geschoten in zijn zorgplicht voor de juistheid van die gegevens.

Artikel 15 Geheimhouding en beveiliging
Artikel 15, eerste lid
Uitgangspunt is dat de verantwoordelijke verantwoordelijk en aansprakelijk is voor de gegevensverwerking. Deze verantwoordelijkheid kan hij slechts dragen wanneer zijn ondergeschikten of degenen die in opdracht van de verantwoordelijke gegevens verwerken, zich naar zijn aanwijzingen richten.

In beginsel kan slechts een uitdrukkelijke wettelijke bepaling op de geheimhoudingsplicht een inbreuk maken. Daarnaast kan de geheimhouding worden doorbroken voor zover uit de taak van de betreffende persoon de noodzaak tot mededeling voortvloeit. Of een noodzaak tot mededeling aanwezig is, wordt bepaald door de verantwoordelijke onder wiens gezag of in wiens opdracht de persoon werkzaam is. Uiteraard is deze bevoegdheid van de verantwoordelijke evenmin onbegrensd. De verantwoordelijke is immers op zijn beurt gehouden aan regels inzake doelbinding en verenigbaar gebruik.

Artikel 15 tweede lid
De beveiligingsverplichting strekt zich uit tot onderdelen van het proces van gegevensverwerking. In het begrip *'passende'* ligt besloten dat de beveiliging in overeenstemming is met de stand van de techniek. Het is niet aan de wetgever om nadere details te geven over de aard van de beveiliging. Dergelijke details zouden sterk tijdgebonden zijn en daarmee afbreuk doen aan het nagestreefde niveau van beveiliging. Het begrip *'passend'* duidt mede op een *proportionaliteit* tussen *de beveiligingsmaatregelen* en *de aard van de te beschermen gegevens.* Naarmate bijvoorbeeld de gegevens een gevoeliger karakter hebben, worden zwaardere eisen gesteld aan de beveiliging van de gegevens. Er is geen verplichting om steeds de allerzwaarste beveiliging te nemen.
Technische en organisatorische maatregelen dienen cumulatief te worden getroffen. Software is een belangrijk instrument tot beveiliging. Klassieke technische beveiligingsmaatregelen omvatten mede de fysieke afscherming van de randapparatuur die toegang geeft tot de te beveiligen gegevens. Daarnaast zijn er de modernere informatietechnologische maatregelen zoals beveiliging door middel van een password.

Artikel 16 Bewaren van persoonsgegevens
De verantwoordelijke dient zich af te vragen of er redenen zijn op grond waarvan gegevens vastgelegd kunnen blijven. Zijn er voldoende redenen dan kan hij bepalen welke termijnen gelden om die

gegevens te bewaren. Zijn die termijnen verlopen dan zal hij de gegevens niet meer mogen verwerken, tenzij voor een ander, daarmee verenigbaar doel. In voorkomende gevallen kunnen in de bijzondere wetgeving nadere regels worden gesteld, zo moeten belastinggegevens in principe zeven jaar bewaard worden (artikel 52 lid 4 AWR); medische gegevens kunnen over het algemeen tien jaar bewaard blijven (artikel 7: 454 lid 3 BW.

In z'n algemeenheid zijn personeelsdossiers in zijn geheel vernietigbaar 10 jaar na het einde van het dienstverband, dan wel 5 jaar na pensionering of 5 jaar na overlijden. Het langer bewaren van persoonsgegevens kan nodig zijn vanwege de administratieve functie, financiële verantwoording of bewijsvoering.
In specifieke omstandigheden kunnen er doeleinden zijn waardoor persoonsgegevens voor onbepaalde tijd mogen worden bewaard. In dit verband kan worden gewezen op de archiefbescheiden als bedoeld in de Archiefwet 1995 die naar een archiefbewaarplaats zijn overgebracht. Voor deze bescheiden geldt onder meer als doeleinde: behoud van (een deel van) het Nederlandse culturele erfgoed. Daarmee is de termijn gedurende welke de daarin opgenomen persoonsgegevens mogen worden bewaard, in beginsel onbepaald.

Artikel 17 Gebruik persoonsgegevens voor onderzoek en statistiek

Voor specifieke historische, statistische of wetenschappelijke doeleinden mogen persoonsgegevens voor onbepaalde tijd worden bewaard. In dit verband kan worden gewezen op de archiefbescheiden als bedoeld in de Archiefwet 1995 die naar een archiefbewaarplaats zijn gebracht. Voor deze bescheiden geldt onder meer als doeleinde: behoud van (een deel van) het Nederlandse culturele erfgoed. Daarmee is de termijn gedurende welke de daarin opgenomen persoonsgegevens mogen worden bewaard in beginsel onbepaald.

Bijlage 1

Bestanden	**Beheer overgedragen aan**
Alle standaard personeelsgegevens WML	Hoofd OPJ
Loongegevens WML	Controller
Financiële gegevens WML	Controller
Bedrijfsvoeringgegevens WML	Controller

Derdengegevens:

Personeelsgegevens	Hoofd OPJ
Loongegevens	Controller
Financiële gegevens	Controller
Bedrijfsvoeringgegevens	Controller

Bijlage 3
Soorten gegevens:
De personeelsregistratie bevat hoofdzakelijk die gegevens zoals hieronder vermeld:

- naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer, e-mailadres, faxnummer, bank- en girorekeningnummer, eventueel ziekenfondsnummer, sociaal fiscaal nummer, burgerlijke staat, partnergegevens en gegevens van eventuele kinderen;
- naam, voorletters, adres, postcode, woonplaats, telefoonnummer, bank- en girorekeningnummer van de ouders, voogden of verzorgers van minderjarige werknemers;
- naam, voorletters, adres, postcode, woonplaats, telefoonnummer van contactpersoon bij alleenstaande werknemer;
- een administratienummer;
- het aanmeldingsformulier voor toelating tot de Wsw, het intakerapport, het door de indicatiecommissie vastgestelde intakeprofiel en eventuele plaatsings- en opleidingsadviezen vanuit deze commissie alsmede het besluit van het bestuur tot toelating tot de Wsw;
- de aanmelding door de gemeente van een Wiw-kandidaat met een Wiw-verklaring;
- het besluit van de gemeente dat een persoon behoort tot de doelgroep van de Wet Rea;
- kopie inschrijving CWI;
- gegevens betreffende het arbeidsverleden;
- gegevens met betrekking tot het wachtlijstbeheer in het kader van de Wsw;
- kopie van de arbeidsovereenkomst met WML ofwel reguliere werkgever;
- gegevens omtrent loon en andere inkomsten, inhoudingen, loonbeslagen, spaarregelingen;
- gegevens betreffende de functie, alsmede betreffende de aard, inhoud, wijzigingen en beëindiging van het dienstverband;
- gegevens betreffende de (secundaire) arbeidsvoorwaarden;
- gegevens, waaronder begrepen gegevens betreffende gezinsleden en voormalige gezinsleden van betrokkenen, voor zover die overigens noodzakelijk zijn met het oog op een overeengekomen arbeidsvoorwaarde;
- gegevens betreffende gevolgde en te volgen opleidingen, cursussen en stages en eventueel behaalde diploma's en getuigschriften;
- rapporten van deskundigen (o.a. psychologisch, medisch)
- gegevens betreffende personeelsbeoordeling en de loopbaanbegeleiding die noodzakelijk zijn met het oog op het organiseren daarvan of die bij betrokkenen bekend zijn (o.a. trajectplannen en voortgangsrapportages);
- gegevens die in het belang van het functioneren van betrokkene worden opgenomen en die redelijkerwijs noodzakelijk zijn met het oog op een goede functievervulling dan wel hun arbeidsomstandigheden;
- gegevens, niet zijnde medische gegevens, die noodzakelijk zijn voor de administratie van de aanwezigheid van de betrokkenen op de plaats waar de arbeid wordt verricht en hun afwezigheid in verband met ziekte, verlof of arbeidsduurverkorting;
- rapportages in het kader van het verzuim, eigen verklaringen, arbeidsongeschiktheidsverklaringen en andere adviezen van de bedrijfsarts;
- besluiten en rapportages in het kader van de herindicatie Wsw;
- gegevens met betrekking tot gevoerde gerechtelijke procedures;
- gegevens met betrekking tot opgelegde disciplinaire maatregelen;
- ontslagadviezen;
- nationaliteit en geboorteplaats van de werknemer en zijn ouders;
- kopie geldig identiteitsbewijs;
- alle gegevens noodzakelijk voor een goede uitvoering van de Wet sociale werkvoorziening, de Wet inschakeling werkzoekenden, de Wet reïntegratie arbeidsgehandicapten en het Besluit In- en Doorstroombanen;

- alle gegevens noodzakelijk voor de uitvoering van werkzaamheden in opdracht van het bestuur;
- alle gegevens noodzakelijk voor de uitvoering van een effectief, efficiënt en sociaal verantwoord personeelsbeleid en –beheer;
- andere dan de genoemde gegevens waarvan de opneming wordt vereist ingevolge of noodzakelijk is met het oog op de toepassing van een wettelijk voorschrift;
- alle overige gegevens waarvoor de betrokkene toestemming geeft tot opneming in het dossier.

2

Wijzen van gegevensverkrijging:

- rechtsreeks van de betrokken personen mondeling of schriftelijk;
- op verzoek van WML of door eigen onderzoek of bevindingen;
- voortvloeiend uit de toepassing van de Wet sociale werkvoorziening, de Wet inschakeling werkzoekenden, de Wet reïntegratie arbeidsgehandicapten en/of het Besluit In- en Doorstroombanen binnen WML;
- middels het inwinnen van informatie bij derden, na daartoe door de betrokkene verleende machtiging, voor zover deze informatieverstrekking door derden niet voortvloeit uit een wettelijk voorschrift dan wel uit het doel waarvoor de derde de gegevens heeft geregistreerd;
- voortvloeiend uit de toepassing van de verschillende rechtspositieregelingen welke van toepassing zijn.

Bijlage 4
Machtiging

MACHTIGING

Het Hoofd van de afdeling Organisatie, Personeel en Juridische zaken (beheerder) en de Controller (beheerder) machtigen de volgende functionarissen (gebruikers), namens hen gegevens uit het personeelsregistratiesysteem te verwerken, voorzover zij deze gegevens in verband met een goede uitvoering van hun taak behoeven.

Gebruikers
Algemeen directeur
Manager divisie diensten
Manager divisie industrie
Beleidsmedewerker Personeel & Organisatie
Beleidsmedewerker Juridische zaken
Bedrijfsmaatschappelijk werkende
Secretaris
Hoofd afdeling reïntegratie
Hoofd afdeling WSW
Personeelsconsulent
Intercedent/ITB'er
Consulent sociale activering
Consulent begeleid werken
Casemanager indicatie commissie/intaker
(assistent) Uitvoerder/ (assistent) werkleider
Medewerkers van de personeelsadministratie
Medewerkers van de financiële administratie
Medewerkers van de loonadministratie
Medewerkers van het ArbeidsdiagnostischCentrum (ADC)
Applicatiebeheerder personeelszaken
Ziekenbezoeker

Bijlage 5

Huishoudelijk reglement n.a.v. privacyreglement personeelsregistratie WML 2004

Wat zijn persoonsgegevens (artikel 1)

- Persoonsgegevens zijn al die gegevens die mede bepalend zijn voor de beoordeling van iemand in het maatschappelijk verkeer en al die gegevens die herleidbaar zijn tot een natuurlijk persoon.

Doel van het verwerken van persoonsgegevens (artikel 2)

- Voor het kunnen verwerken van persoonsgegevens heeft WML een geldige grondslag c.q. doelstelling geformuleerd zoals vermeld in artikel 2 van het privacyreglement WML.

Actieve informatieplicht WML (artikel 6)

- WML verstrekt aan diegene van wie persoonsgegevens worden geregistreerd adequate informatie over de verwerking en het doel van het verzamelen van diens persoonsgegevens door een korte toelichting hierop te geven in het personeelsinformatieboekje waarover iedere medewerker van WML beschikt. Daarnaast ligt het volledige privacyreglement van WML ter inzage bij de beheerders (hoofd OPJ en de controller) en bij de personeelsadministraties.
- Worden persoonsgegevens direct aan betrokkene gevraagd dan informeert WML betrokkene over het doel hiervan vóór het moment van verkrijging van de benodigde informatie. Deze informatie wordt slechts achterwege gelaten als betrokkene reeds van dit verzamelen op de hoogte is, omdat dit bijvoorbeeld middels een schrijven c.q. brochure aan hem bekend is gemaakt.
- Bij verkrijging van persoonsgegevens buiten betrokkene om, bijvoorbeeld bij derden of door eigen observatie, informeert WML betrokkene indien deze gegevens worden vastgelegd dan wel, indien verstrekking van gegevens aan derden wordt overwogen. Dit informeren vindt plaats uiterlijk op het moment van de eerste verstrekking c.q. vastlegging.

Verwerking en nevengebruik van persoonsgegevens (artikel 7)

- De persoonsgegevens worden na het verzamelen door WML verwerkt op een wijze die behoorlijk is, zorgvuldig is en verenigbaar is met de doeleinden waarvoor ze zijn verkregen.
- Nevengebruik van persoonsgegevens is door WML toegestaan mits dit gebruik met het oorspronkelijke doel van verwerken c.q. verzamelen niet onverenigbaar is.

Verstrekking van persoonsgegevens aan derden (artikel 10)

Persoonsgegevens worden door WML slechts aan derden verstrekt met toestemming van betrokkene of indien verstrekking noodzakelijk is voor de uitvoering van een overeenkomst, voor de uitvoering van een wettelijke verplichting, ter vrijwaring van een vitaal belang, voor de goede invulling van een publiekrechtelijke taak of voor de behartiging van een gerechtvaardigd belang. Van alle verzoeken om verstrekking van gegevens aan derden en de besluitvorming daaromtrent, wordt aantekening gehouden in het dossier.

Inzage van gegevens (artikel 11)

- Betrokkene heeft het recht zich met redelijke tussenpozen te wenden tot zijn personeelsconsulent met het verzoek hem inzage te geven in zijn eigen personeelsdossier.
- Inzage vindt plaats onder begeleiding van de P&O consulent, zonodig kan toelichting worden gegeven.
- Indien betrokkene niet in staat wordt geacht tot een redelijke waardering van zijn belangen terzake, dan treedt een andere persoon als zijn gemachtigde op.
- Van alle verzoeken om inzage en de besluitvorming daaromtrent, wordt aantekening gehouden in het dossier.

Afschrift (artikel 12)

- Bij toestemming tot inzage kan betrokkene, indien hij dit wenst, kopieën laten maken van de aanwezige stukken. Op de kopieën wordt door de P&O consulent (of medewerker personeelsadministratie) aangegeven dat het om een kopie handelt.
- Bij verstrekking van meer dan 100 bladzijden afschriften is WML gerechtigd om de maximale kostprijs in rekening te brengen.
- Van alle verzoeken om een afschrift en de besluitvorming daaromtrent wordt aantekening gehouden in het dossier van betrokkene.

Correctie van gegevens (artikel 14)

- Betrokkene kan na inzage het hoofd OPJ verzoeken zijn persoonsgegevens te verbeteren, aan te vullen, te verwijderen, of af te schermen, indien deze feitelijk onjuist zijn, indien gegevens ontbreken, indien gegevens bovenmatig zijn, indien gegevens in strijd met de wet zijn, of niet meer ter zake dienend zijn.
- Het indienen van een verzoek tot correctie dient schriftelijk te gebeuren bij het hoofd OPJ eventueel met te overleggen bewijsstukken.
- Het hoofd OPJ onderzoekt de juistheid van de gegevens en bericht betrokkene binnen 4 weken na ontvangst van het verzoek of dan wel in hoeverre hij daaraan voldoet.
- Bij een terecht verzoek draagt het hoofd OPJ zorg voor de correctie; een onterecht verzoek wordt met redenen omkleed schriftelijk aan betrokkene medegedeeld.
- Binnen 6 weken na ontvangst van de weigering kan betrokkene een bezwaarschrift indienen bij het dagelijks bestuur van WML.

Beveiligingsmaatregelen (artikel 15) en bijlage 7 van dit reglement

- Een ieder die in het kader van het privacyreglement WML de beschikking krijgt over persoonsgegevens is verplicht tot geheimhouding daarvan, mits enig wettelijk voorschrift hem tot bekendmaking verplicht of de noodzaak tot mededeling uit zijn taak voortvloeit. Tevens dient in acht te worden genomen het protocol "Omgaan met communicatiemiddelen" van WML en de door medewerkers getekende geheimhoudings-gebruikersverklaring voor het werken met het personeelsregistratiesysteem en de geheimhoudingsverplichting zoals deze is opgenomen in de huisregels van WML.
- Technische beveiligingsmaatregelen worden door WML genomen ter voorkoming van onrechtmatige verwerking of verlies van persoonsgegevens.

Bewaren van gegevens (artikel 16) en bijlage 6 van dit reglement

- Gegevens worden door WML in ieder geval niet langer bewaard dan noodzakelijk is voor de doeleinden waarvoor zij zijn verzameld of verder worden verwerkt. Als gegevens niet meer noodzakelijk zijn voor het doel waarvoor zij zijn verzameld, worden ze geanonimiseerd, uit de registratie verwijderd of vernietigd.
- Met "uit de registratie verwijderd" wordt bedoeld dat persoonsgegevens niet langer in de actieve registratie van WML blijven zitten, maar worden overgebracht naar bijvoorbeeld het archief. In het archief krijgen deze gegevens een andere doelbestemming, namelijk historisch, statistisch of wetenschappelijk.
- Betrokkene heeft recht op vernietiging van (delen van) het dossier. Zo'n verzoek kan worden geweigerd indien de gegevens vallen onder de wettelijke bewaarplicht of indien bewaring van de gegevens van aanmerkelijk belang is voor de beheerder. Als betrokkene nog in dienst is, is vernietiging van (delen van) het personeelsdossier niet mogelijk.
- Verzoek tot vernietiging van (delen van) het dossier geschiedt volgens dezelfde procedure als genoemd in artikel 14 lid 2 (procedure voor de uitoefening van het correctierecht).
- Vernietiging op verzoek van betrokkene komt voor diens risico.
- Werkleiding kan uitsluitend verzoeken om kopieën uit het persoonsdossier van zijn/haar medewerkers als deze gegevens NIET in het personeelsregistratiesysteem zijn opgenomen. Kopie gegevens aanwezig bij werkleiding worden in een afsluitbare ruimte (kast, lade) bewaard, zodat deze niet toegankelijk zijn voor anderen. Deze kopie gegevens worden direct na gebruik vernietigd of periodiek door werkleiding overgedragen aan de personeelsadministratie. Na einde dienstverband of bij her/overplaatsing naar een andere divisie/afdeling worden de kopiegegevens opgevraagd door de personeelsadministratie en per direct overgedragen door de werkleiding aan de personeelsadministratie.

Bijlage 6 Checklist algemene bewaartermijnen documenten in personeelsdossiers (zie artikel 16 van het privacyreglement)

De algemene bewaartermijnen van de diverse documenten in het personeelsdossier zijn:

Soort gegevens	**Bewaartermijn**
HUIDIGE AFGESLOTEN DOSSIERS	
• Persoonsdossier individuele personeelsleden	• 10 jaar na uitdiensttreding
• Re-integratietrajecten UWV	• 2 jaar na beëindiging van het re-integratietraject, met uitzondering van de gegevens waarvoor de wettelijke bewaarplicht van 10 jaar geldt.
ACTIEVE DOSSIERS	
• Persoonsdossier individuele personeelsleden	• 10 jaar na uitdiensttreding
• Sollicitatiegegevens van niet benoemde kandidaten	• uiterlijk 4 weken bij niet benoemde sollicitanten • maximaal 1 jaar met schriftelijke toestemming van de kandidaat
• Psychologisch onderzoek voor bepaling geschiktheid voor functie. • Rapporten van medische, en andere deskundigen, ook psychologen in het kader van arbeid(on)geschiktheid/ stoornissen, verstandelijke beperkingen e.d.	• 2 jaar na datum onderzoek • 10 jaar, vallen nl. onder de Wet Geneeskundige Behandelings-overeenkomst (WGBO)
• Beoordelingsformulieren	5 jaar
• Vertrouwelijke gegevens inzake incidenten behandeld door vertrouwenspersonen en de commissie ongewenste omgangsvormen.	10 jaar na datum incident. Bewaren in separaat gesloten archief van de commissie, enkel toegankelijk voor vertrouwenspersonen en voorzitter/secretaris van commissie.
• Wachtlijstgegevens/wachtlijstdossier • Gegevens van kandidaten die niet zijn toegelaten tot de wachtlijst.	• 5 jaar nadat de persoon van de wachtlijst is afgegaan en geen geldige indicatie meer heeft • 5 jaar

Algemeen:

- Nadat een persoon uit dienst is, is het dienstverband administratief afgehandeld, kan het personeelsdossier uit de kast met personeelsleden in dienst worden gehaald en worden afgevoerd naar de archiefruimte.
- Voor re-integratietrajecten UWV is de bewaartermijn 2 jaar na beëindiging van het re-integratietraject, met uitzondering van de gegevens waarvoor de wettelijke bewaarplicht van 10 jaar geldt.
- Na 2 jaar resp. 5 jaar resp. 10 jaar wordt het personeelsdossier en het personeelsregistratiesysteem door het bedrijf ontdaan van een aantal persoonsgegevens op basis van de hierboven wettelijk vastgestelde minimum bewaartermijnen.
- Het personeelsdossier c.q. de gegevens in het personeelsregistratiesysteem worden uiterlijk 10 jaar na einde dienstverband vernietigd.
- Gegevens m.b.t. een sollicitatie worden op verzoek van de kandidaat direct (uiterlijk binnen 4 weken) vernietigd, tenzij de kandidaat schriftelijk toestemming geeft om deze maximaal 1 jaar te bewaren.
- De psychologische rapporten dienen in het persoonsdossier te worden bewaard, waarbij de P&O consulent op dit rapport vermeldt:
  a. of het onderzoek is voor bepaling geschiktheid van een functie of een medisch onderzoek/ onderzoek naar verstandelijke beperking;
  b. en datum vernietiging van het onderzoek;
- Kopiegegevens werkleiding: Werkleiding kan uitsluitend verzoeken om kopieën uit het persoonsdossier van zijn/haar medewerker als deze gegevens NIET in het personeelsregistratiesysteem zijn opgenomen. Kopie persoonsgegevens bij werkleiding aanwezig worden in een afsluitbare ruimte (lade, kast), niet toegankelijk voor anderen, bewaard, en tijdens het dienstverband direct na gebruik vernietigd of periodiek door werkleiding overgedragen aan de personeelsadministratie. Na einde dienstverband of bij her/overplaatsing naar andere afdeling/divisie worden de kopiegegevens bij werkleiding opgevraagd door de personeelsadministratie en door werkleiding per direct overgedragen.

Bijlage 7 Checklist beveiliging persoonsgegevens (artikel 15 van het privacyreglement)

A. Toegankelijkheid personeelsregistratiesysteem en persoonsdossier

1.a. Conform artikel 11 van het reglement heeft betrokkene zelf het recht zich vrijelijk en met redelijke tussenpozen te wenden tot de personeelsconsulent om inzage te verkrijgen in de persoonsgegevens die over hem worden verwerkt.

1.b. Deze inzage vindt te allen tijde plaats onder begeleiding van de P&O consulent.

1.c. Van alle verzoeken tot inzage wordt aantekening bijgehouden in het dossier.

2. De gebruikers, zoals deze zijn opgesomd in bijlage 2 van het reglement, hebben in het personeelsregistratiesysteem en met betrekking tot de persoonsgegevens in het persoonsdossier, uitsluitend inzage in de persoonsgegevens van de opgesomde categorieën van betrokkenen, zoals deze zijn genoemd in bijlage 2 van het reglement.

B. Beveiliging persoonsgegevens

1.a. Een ieder die de beschikking krijgt over persoonsgegevens is te allen tijde verplicht tot geheimhouding daarvan.

1.b. Een ieder die uit hoofde van zijn functie inzicht krijgt in persoonsgegevens tekent bij in dienst name de geheimhoudings- gebruikersverklaring Compas, zoals opgenomen in het handboek OPJ.

2. Wanneer ongevraagd persoonsgegevens van medewerkers van WML komen bij personen binnen of buiten de organisatie van WML dienen deze terstond te worden overgedragen aan directie van WML of de werkleiding.

3. Kantoren, kasten, archiefruimten, bureaulades, personeelsbakjes en overige ruimten/zaken binnen de organisatie waar zich persoonsgegevens bevinden, dienen afsluitbaar te zijn. Indien de hierin aanwezige persoonsgegevens op een bepaald moment van de dag niet meer actief worden gebruikt, dienen genoemde zaken en/of ruimten afgesloten te zijn en hierdoor niet toegankelijk voor onbevoegden.

4.a. Achiefruimten waar zich persoonsgegevens bevinden zijn afsluitbaar en uitsluitend toegankelijk voor medewerkers van de afdeling Organisatie, Personeel en Juridische zaken (OPJ) en medewerkers van F&A m.b.t. de financiële gegevens.

4.b. De archiefruimte met hierin de dossiers van de Commissie Ongewenste Omgangsvormen is uitsluitend toegankelijk voor de vertrouwenspersonen van WML en de secretaris en voorzitter van de genoemde commissie.

4.c. De archiefruimte met daarin de bestuursstukken is uitsluitend toegankelijk voor het directiesecretariaat.

5.a. De persoonsdossiers in de archiefkasten, zoals deze aanwezig zijn op de personeelsadministraties binnen WML, kunnen uitsluitend tijdelijk worden meegenomen (na het invullen van de “rode kaart”) door medewerkers van de afdeling organisatie, personeel en juridische zaken (OPJ), P&O consulenten en medewerkers van de afdeling reïntegratie, uitsluitend met betrekking tot persoonsdossiers van de personen in een reïntegratietraject.

5.b. Indien door werkleiding wordt verzocht om één van de dossiers van zijn/haar medewerkers, kunnen deze uitsluitend worden ingekeken bij de desbetreffende personeelsadministratie, waar dit dossier aanwezig is. Dit dossier mag dus niet door werkleiding worden meegenomen. Het meenemen van het persoonsdossier door werkleiding naar de werkplek mag uitsluitend geschieden met de uitdrukkelijk verkregen toestemming van het HOPJ.

6.a. Werkleiding kan uitsluitend verzoeken om kopieën uit het persoonsdossier van zijn/haar medewerkers die betrekking hebben op relevante gegevens die NIET vermeld zijn in het personeelsregistratiesysteem.

6.b. Deze kopieën worden in een dergelijk geval door medewerkers van de personeelsadministratie gemaakt.

6.c. Kopieën inzake persoonsgegevens die bij werkleiding aanwezig zijn worden in een afsluitbare ruimte (kast, lade), niet toegankelijk voor anderen, bewaard, en worden tijdens het dienstverband direct na gebruik vernietigd of tenminste periodiek door werkleiding overgedragen aan de P&O consulent.

6.d. De personeelsadministratie vraagt na het einde dienstverband of bij her/overplaatsing naar een andere afdeling/divisie de kopiegegevens op bij de werkleiding, die door werkleiding per direct worden overgedragen aan personeelsadministratie.

7.a. De beheerder, systeembeheerder en applicatiebeheerder dragen zorg voor het aanleggen van passende maatregelen om persoonsgegevens in het personeelsregistratiesysteem te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking o.a. door het gebruik van (en het jaarlijks wisselen van) pass-words, het beveiligd bewaren van elektronische informatiedragers, het uitvoeren van een back-up procedure ter voorkoming van het verlies van gegevens en het aanleggen van gebruikersprofielen voor gebruikers, zoals blijkt uit punt A2 (bijlage 2 van het privacyreglement).

7.b. De met enige regelmaat door de afdeling I&A uit te voeren back-ups met personeelsinformatie worden tot uiterlijk 10 jaar na uitvoering bewaard en daarna door I&A vernietigd.

Bijlage 2. Algemene meldplicht

Inhoud van de melding
In artikel 28 Wbp is bepaalt dat de inhoud van de algemene melding bestaat uit:[1]

- **Identiteit van de verantwoordelijk (de naam en het adres);**
  De identiteit en gegevens waarmee de verantwoordelijke te contacteren is zijn nodig om met hem te kunnen communiceren.
- **Doel of de doeleinden van de verwerking;**
- **Categorieën van betrokkenen en de omtrent hen te verwerken gegevens;**
- **De ontvangers van de gegevens;**
  Het gaat hierbij zowel om gevallen waarin gegevens zijn verstrekt naar derden als om gevallen waarin deze gegevens zijn verstrekt aan personen of afdelingen binnen de organisatie. Hiermee wordt duidelijk weergeven hoe de gegevens worden verwerkt.
- **Gegevensoverdracht naar landen buiten de EU**
- **Algemene beschrijving van de beveiligingsmaatregelen**
- **Het doel of de doeleinden waarvoor de gegevens zijn verzameld**
- **Melding van wijzigingen**
  Een wijziging in de naam of het adres van de verantwoordelijke wordt binnen een week gemeld.[2]
- **Incidentele wijzigingen**
  Alleen wijzigingen die niet regelmatig voorkomen dienen gemeld te worden.
- **Structurele wijzigingen**
  Hieraan wordt achteraf getoetst.

De daadwerkelijke verwerking van de persoonsgegevens mag pas plaatsvinden wanneer de verantwoordelijke daarvoor de ontvangstbevestiging met het meldingsnummer van de Autoriteit Persoonsgegevens heeft gekregen.[3]

Register gegevensverwerkingen
In artikel 30 is geregeld dat zowel de Autoriteit Persoonsgegevens als de functionaris de aangemelde gegevensverwerkingen bijhouden in een register. Daarbij wordt de inhoud van de melding ingevolge artikel 28 Wbp in het register opgenomen. De meldingen die in het register zijn opgenomen zijn openbaar, waardoor wordt voldaan aan het transparantiebeginsel.

Termijn inlichtingenplicht verantwoordelijke
Voorgesteld wordt om een termijn van vier weken te hanteren voor de inlichtingenplicht van de verantwoordelijke.[4] Indien de inlichtingen niet binnen vier weken kunnen worden gegeven, dan stelt de verantwoordelijke de aanvrager daarvan in kennis en noemt hij daarbij een kort mogelijke termijn waarbinnen de inlichtingen wel tegemoet kunnen worden gezien.[5]

Verplichtingen waarvoor een boete kan worden opgelegd, zijn:[6]

- Het niet tijdig en op juiste wijze melden van de gegevensverwerking;
- Het niet verstrekken van de juiste en volledige informatie omtrent de gegevensverwerking;
- Het niet tijdig melden van wijzigingen in de opgaven bij de oorspronkelijke melding;
- Het niet bewaren van gegevens omtrent de gewijzigde verwerking.

---

[1] T.F.M. Hooghiemstra en S. Nouwt, *'Sdu Commentaar Wet bescherming persoonsgegevens'*, Sdu Uitgevers 2012, pagina 118.
[2] Artikel 28 lid 3 Wbp
[3] E.Thole, F. van der Jagt en H. Roerdink, *'50 vragen over privacy'*, Wolters Kluwer uitgevers 2010, pagina 99.
[4] Kamerstukken II 2009/10, 31 841, nr. 13
[5] T.F.M. Hooghiemstra en S. Nouwt, *'Sdu Commentaar Wet bescherming persoonsgegevens'*, Sdu Uitgevers 2012, pagina 125.
[6] E.Thole, F. van der Jagt en H. Roerdink, *'50 vragen over privacy'*, Wolters Kluwer uitgevers 2010, pagina 106.

Vrijstelling meldplicht

Artikel 29 lid 1 Wbp bepaalt dat niet alle persoonsgegevens dienen te worden gemeld. Gegevens waarvan bekend is dat het kan voorkomen dat deze worden verwerkt en waarvan de inbreuk op de op de persoonlijke levenssfeer onwaarschijnlijk is, zijn van de meldingsplicht vrij te stellen. De persoonsgegevens die in aanmerking komen voor de vrijstelling zijn opgenomen in het Vrijstellingsbesluit.[7] Daarin staat precies vermeld welke gegevens onder de vrijgestelde verwerking vallen, wat het doel is, wat het gebruik is en bijvoorbeeld aan wie ze mogen worden verstrekt.[8]

Inlichtingen over vrijgestelde gegevensverwerkingen kan eenieder (en dus niet alleen de betrokkene) verkrijgen bij de verantwoordelijke. Iedere verantwoordelijke dient desgevraagd inlichtingen te verstrekken over door hem verwerkte persoonsgegevens voor zover het gaat om vrijgestelde verwerkingen.[9] Het verzoek on inlichtingen te verstrekken dient door de degene die inlichtingen daarover wil hebben met precisie te worden gedaan, zodat wordt voorkomen dat de verantwoordelijke onevenredige inspanning vergt. Wordt hier niet aan voldaan, dan kan de verantwoordelijke het verzoek terzijde leggen, omdat de verzoeker misbruik maakt van het recht. De verantwoordelijke kan zich dan beroepen op het feit dat ‘een gewichtig belang aan zijn kant een inwilliging van het verzoek in de weg staat’[10].

De verantwoordelijke zal zelf aan de hand van het ‘Vrijstellingsbesluit’ moeten beoordelen of hij in aanmerking komt voor één of meer vrijstellingen. Bij twijfel is het raadzaam om toch tot melding over te gaan.

[7] Vrijstellingsbesluit Wbp
[8] mr. S.M. Huydecoper, *‘Wet bescherming en persoonsgegevens en ICT’,* Sdu Uitgevers 2006, pagina 44.
[9] T.F.M. Hooghiemstra en S. Nouwt, *‘Sdu Commentaar Wet bescherming persoonsgegevens’*, Sdu Uitgevers 2012, pagina 124.
[10] Artikel 43 onderdeel e Wbp

Bijlage 3. Nadere toelichting over omtrent de meldplicht datalekken

Wat is een datalek?
Er is sprake van een datalek als persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens zouden mogen hebben.[1] Artikel 34a lid 1 Wbp stelt dat het moet gaan om gegevens waarbij het verlies daarvan "leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens." Kan niet worden uitgesloten dat als gevolg van het verlies de persoonsgegevens onrechtmatig zijn aangetast, dan wordt de inbreuk ook beschouwd als een datalek.[2] Onder onrechtmatige vormen van verwerking vallen de aantasting van de persoonsgegevens, onbevoegde kennisneming, wijziging, of verstrekking daarvan.[3]
Een datalek is het gevolg van een inbreuk op de *passende technische en organisatorische maatregelen en passend beveiligingsniveau. Deze beveiliging dient namelijk tot het voorkomen van datalek. Bij een datalek betekent het dat er dan* daadwerkelijk een beveiligingsincident heeft voorgedaan en de preventieve maatregelen die eventueel zijn getroffen waren niet toereikend om dit te voorkomen.[4]

Praktische voorbeelden[5] van incidenten, die zouden kunnen voorkomen bij een organisatie en waarbij sprake kan zijn van een datalek, zoals omschreven in artikel 34a Wbp zijn:
- Het kwijtraken van een usb met (gevoelige) persoonsgegevens van betrokkene;
- Een inbraak in de pc's door een hacker;
- Verzending van e-mail waarin de e-mailadressen van alle geadresseerden zichtbaar zijn voor alle andere geadresseerden;
- Malware (kwaadaardige software);
- Het onjuist bewaren van identiteitsgegevens;
- Een calamiteit zoals een brand in een datacentrum.

De Autoriteit Persoonsgegevens heeft beleidsregels[6] opgesteld, op grond waarvan de verantwoordelijke kan beoordelen of er sprake is van een datalek en of dit gemeld moet worden.

Wanneer en hoe wordt een datalek gemeld?
Er hoeft geen melding te worden gemaakt van iedere datalek. Het datalek dient gemeld te worden als het gevolg van het verlies voldoet aan de criteria van artikel 34a lid 1 Wbp. Namelijk dat de inbreuk redelijkerwijs leidt tot "de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens." Daarbij moet ook rekening gehouden worden met of de persoonsgegevens van gevoelige aard zijn. Een melding is dan namelijk noodzakelijk. Onder gevoelige persoonsgegevens vallen o.g.v. de beleidsregels in ieder geval:[7]
- Bijzondere persoonsgegevens zoals bedoeld in artikel 16 Wbp;
- Gegevens over de financiële of economische situatie van de betrokkene;
- (Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene;
  (prestaties op school, verslavingen, werk of relatieproblemen);
- Gebruikersnamen, wachtwoorden en andere inloggegevens;
- Gegevens die kunnen worden misbruikt voor (identiteits)fraude,

[1] 'Datalekken', www.justitia.nl (zoek op *meldplicht datalekken procedure*)
[2] *Kamerstukken II* 2014/15, 33 662, nr. 11, pagina 4.
[3] Beleidsregels voor toepassing van artikel 34a van de Wbp, pagina 21.
[4] Beleidsregels voor toepassing van artikel 34a van de Wbp, pagina 19.
[5] Beleidsregels voor toepassing van artikel 34a van de Wbp, pagina 21.
[6] Beleidsregels voor toepassing van artikel 34a van de Wbp 2015.
[7] Beleidsregels voor toepassing van artikel 34a van de Wbp, pagina 5.

De melding moet gedaan worden zonder onnodige vertraging en zo mogelijk niet later dan 72 uur na de ontdekking van het datalek.[8] Indien 72 uur na de ontdekking van het incident nog niet volledig zicht is op wat er is gebeurd en om welke persoonsgegevens het gaat, wordt een melding gedaan op basis van de gegevens waarover de verantwoordelijke op dat moment beschikt.[9] Naderhand kan de melding worden aangevuld of ingetrokken. De melding kan via de webformulier, dat op de website van de Autoriteit Persoonsgegevens beschikbaar staat, worden gedaan.

Door wie en aan wie wordt een datalek gemeld?
De verantwoordelijk is verplicht onverwijld en zo mogelijk binnen 72 uur, nadat hij op de hoogte is van het datalek een melding te doen bij de Autoriteitspersoonsgegevens.[10] Op grond van artikel 34a lid 2 Wbp dient de verantwoordelijke in sommige gevallen ook de betrokkene in kennis te stellen van het datalek, indien het datalak ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer. Ingeval van een datalek van persoonsgegevens die van gevoelige aard zijn, dient de betrokkene daar van op de hoogte te worden gesteld. De melding stelt de betrokkene in staat om alert te zijn op de mogelijke gevolgen van het datalek en om zich daar waar mogelijk tegen te wapenen, door bijvoorbeeld een gelekt wachtwoord te vervangen.[11]

Inhoud van de melding
De melding aan de Autoriteitspersoonsgegevens omvat in ieder geval de aard van de inbreuk, het contactpunt waar meer informatie kan worden verkregen en de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken.[12] De kennisgeving omvat tevens een beschrijving van de geconstateerde en de vermoedelijke gevolgen van de inbreuk voor de verwerking van persoonsgegevens en de maatregelen die de verantwoordelijke heeft getroffen of voorstelt te treffen om deze gevolgen te verhelpen.[13] Over de inhoud van de kennisgeving aan de betrokkene is in artikel 43a lid 4 Wbp geregeld dat het op een zodanige wijze moet worden gedaan dat een behoorlijke en zorgvuldige informatievoorziening is gewaarborgd.

Boetebevoegdheid
Om de naleving van de Wbp te stimuleren heeft de Autoriteit Persoonsgegevens een sterke boetebevoegdheid gekregen. De boetebevoegdheid bestaat uit een hoge bestuurlijke boete die wordt opgelegd bij niet naleving van de Wbp. Per 1 januari 2016 is de boete maximaal 820.000 euro.[14] Voor het bepalen van de hoogte van de boete zijn de artikelen van de Wbp ingedeeld in categorie 1, 2 of 3. De Autoriteit Persoonsgegevens zal daarbij rekening houden met omstandigheden van het geval, zodat de sanctie in verhouding staat met de begane overtreding. Indien de overtreding niet opzettelijk is gepleegd en er geen sprake is van ernstig verwijtbare nalatigheid, dan zal de Autoriteit Persoonsgegevens eerst een bindende aanwijzing opleggen voorafgaand aan eventuele oplegging van een bestuurlijke boete.[15] Als sprake is van een overtreding van de Wbp die opzettelijk is gepleegd of het gevolg is van ernstig verwijtbare nalatigheid, kan de toezichthouder direct een bestuurlijke boete opleggen.[16]

Gevolgen (onrechtmatig nalaten) melding datalek
Indien de verantwoordelijke het datalek niet meldt aan de betrokkene kan de Autoriteit Persoonsgegevens ingeval van ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene, verlangen van de verantwoordelijk om alsnog een kennisgeving te doen aan de

[8] Beleidsregels voor toepassing van artikel 34a van de Wbp, pagina 6.
[9] Beleidsregels voor toepassing van artikel 34a van de Wbp, pagina 32.
[10] Artikel 43a lid 2 Wbp
[11] Beleidsregels voor toepassing van artikel 34a van de Wbp, pagina 6.
[12] Artikel 43a lid 3 Wbp
[13] Artikel 43a lid 4 Wbp
[14] Artikel 23 lid 4 Wetboek van Strafrecht
[15] Beleidsregels voor toepassing van artikel 34a van de Wbp, pagina 7.
[16] Artikel 66 lid 4 Wbp

betrokkene. Dit is bepaald in artikel 34a lid 7 Wbp. Dit is een bindende aanwijzing. Komt de verantwoordelijke deze niet na, dan kan de Autoriteit Persoonsgegevens een bestuurlijke boete opleggen van ten hoogste het bedrag van de geldboete van de zesde categorie. [17]

[17] Categorie uit artikel 23 lid 4 Wetboek van Strafrecht

Bijlage 4. Boetebeleidsregels

Beleidsregels van het College bescherming persoonsgegevens van [*datum*] met betrekking tot het opleggen van bestuurlijke boetes (Boetebeleidsregels Autoriteit Persoonsgegevens 2015)

Het College bescherming persoonsgegevens heeft, gelet op artikel 4:81 van de Algemene wet bestuursrecht, artikel 66 van de Wet bescherming persoonsgegevens, artikel 35, derde lid, van de Wet politiegegevens, artikel 27, vierde lid, van de Wet justitiële en strafvorderlijke gegevens en artikel 15.4, vierde lid, van de Telecommunicatiewet, besloten om de volgende beleidsregels met betrekking tot het bepalen van de hoogte van bestuurlijke boetes vast te stellen:

Hoofdstuk 1. Algemene bepalingen

Artikel 1. Definities

In deze beleidsregels wordt verstaan onder:

a. *Autoriteit Persoonsgegevens*: het College bescherming persoonsgegevens, genoemd in artikel 51 van de Wet bescherming persoonsgegevens;
b. *basisboete*: het bedrag dat de basis vormt voor het bepalen van de hoogte van een op te leggen bestuurlijke boete, vastgesteld binnen de bandbreedte van de aan een overtreding gekoppelde boetecategorie, voordat toepassing is gegeven aan de paragrafen 2.4 en 2.5;
c. *betrokkene*: degene op wie een persoonsgegeven betrekking heeft als bedoeld in artikel 1, aanhef en onder f, van de Wet bescherming persoonsgegevens.

Hoofdstuk 2. Bepalen van de hoogte van bestuurlijke boetes

Paragraaf 2.1 Overtredingen met een wettelijk boetemaximum van € 810.000

Artikel 2. Categorie-indeling en boetebandbreedtes

2.1 De bepalingen ter zake van overtreding waarvan de Autoriteit Persoonsgegevens een bestuurlijke boete van ten hoogste het bedrag van de geldboete van de zesde categorie van artikel 23, vierde lid, van het Wetboek van Strafrecht (per 1 januari 2014: € 810.000)[1] kan opleggen, zijn in bijlage 1 ingedeeld in categorie I, categorie II of categorie III.

2.2 De Autoriteit Persoonsgegevens stelt de basisboete voor overtredingen waarvoor een wettelijk boetemaximum van € 810.000 geldt vast binnen de volgende boetebandbreedtes:

Categorie I	Boetebandbreedte tussen € 0 en € 200.000
Categorie II	Boetebandbreedte tussen € 120.000 en € 500.000
Categorie III	Boetebandbreedte tussen € 350.000 en € 810.000

Paragraaf 2.2 Overtredingen met een wettelijk boetemaximum van € 450.000

Artikel 3. Categorie-indeling en boetebandbreedtes

3.1 De bepalingen ter zake van overtreding waarvan de Autoriteit Persoonsgegevens een

[1] Zie artikel I van het Besluit van 17 oktober 2013 tot wijziging van de bedragen van de categorieën, bedoeld in artikel 23, vierde lid, van het Wetboek van Strafrecht (*Stb.* 2013, nr. 420).

bestuurlijke boete van ten hoogste het bedrag van € 450.000 kan opleggen, zijn in bijlage 2 ingedeeld in categorie I, categorie II of categorie III.

3.2 De Autoriteit Persoonsgegevens stelt de basisboete voor overtredingen waarvoor een wettelijk boetemaximum van € 450.000 geldt vast binnen de volgende boetebandbreedtes:

Categorie I	Boetebandbreedte tussen € 0 en € 100.000
Categorie II	Boetebandbreedte tussen € 60.000 en € 300.000
Categorie III	Boetebandbreedte tussen € 200.000 en € 450.000

Paragraaf 2.3 Overtredingen met een wettelijk boetemaximum van € 20.250

Artikel 4. Categorie-indeling en boetebandbreedtes

4.1 De bepalingen ter zake van overtreding waarvan de Autoriteit Persoonsgegevens een bestuurlijke boete van ten hoogste het bedrag van de geldboete van de vierde categorie van artikel 23, vierde lid, van het Wetboek van Strafrecht (per 1 januari 2014: € 20.250)[2] kan opleggen, zijn in bijlage 3 ingedeeld in categorie I of categorie II.

4.2 De Autoriteit Persoonsgegevens stelt de basisboete voor overtredingen waarvoor een wettelijk boetemaximum van € 20.250 geldt vast binnen de volgende boetebandbreedtes:

Categorie I	Boetebandbreedte tussen € 0 en € 12.500
Categorie II	Boetebandbreedte tussen € 7.500 en € 20.250

Paragraaf 2.4 Bepalen van de hoogte van de boete

Artikel 5. De basisboete en mogelijke verhoging of verlaging

De Autoriteit Persoonsgegevens bepaalt de hoogte van de boete door het bedrag van de basisboete naar boven (tot ten hoogste het maximum van de bandbreedte) of naar beneden (tot ten laagste het minimum van de bandbreedte) bij te stellen. De basisboete wordt verhoogd of verlaagd afhankelijk van de mate waarin de factoren die zijn genoemd in artikel 6 daartoe aanleiding geven.

Artikel 6. Relevante factoren

6.1 De Autoriteit Persoonsgegevens stemt de beoordeling van de ernst van de overtreding in het concrete geval af op:
   a. de aard en omvang van de overtreding;
   b. de duur van de overtreding;
   c. de impact van de overtreding op (de bescherming van persoonsgegevens en van de persoonlijke levenssfeer voor) de betrokkenen en/of de maatschappij.

6.2 De Autoriteit Persoonsgegevens houdt bij de beoordeling van de concrete omstandigheden van het geval rekening met de mate waarin de overtreding aan de overtreder kan worden

[1] Zie artikel I van het Besluit van 17 oktober 2013 tot wijziging van de bedragen van de categorieën, bedoeld in artikel 23, vierde lid, van het Wetboek van Strafrecht (*Stb.* 2013, nr. 420).

verweten. Indien de overtreding opzettelijk is gepleegd of het gevolg is van ernstig verwijtbare nalatigheid als bedoeld in artikel 66, vierde lid, van de Wet bescherming persoonsgegevens, wordt aangenomen dat sprake is van een aanzienlijke mate van verwijtbaarheid van de overtreder.

6.3 De Autoriteit Persoonsgegevens houdt zo nodig rekening met de omstandigheden waaronder de overtreding is gepleegd en de (financiële) omstandigheden waarin de overtreder verkeert.

Artikel 7. Buiten de bandbreedte treden

7.1 Indien de voor de overtreding bepaalde boetecategorie in het concrete geval geen passende bestraffing toelaat, kan de Autoriteit Persoonsgegevens bij het bepalen van de hoogte van de basisboete de boetebandbreedte van de naast hogere categorie respectievelijk de bandbreedte van de naast lagere categorie toepassen.

7.2 Indien ter zake van de overtreding aan een rechtspersoon een boete van € 810.000 kan worden opgelegd en dit boetemaximum naar het oordeel van de Autoriteit Persoonsgegevens geen passende bestraffing toelaat, kan zij een boete opleggen tot ten hoogste tien procent van de jaaromzet van de rechtspersoon in het boekjaar voorafgaande aan het besluit waarbij de boete wordt opgelegd. Onder jaaromzet van de rechtspersoon wordt verstaan de netto-omzet, bedoeld in artikel 377, zesde lid, van boek 2 van het Burgerlijk Wetboek, die de overtreder heeft behaald in het meest recente boekjaar ten aanzien waarvan de overtreder een jaarrekening beschikbaar heeft of zou moeten hebben.

Paragraaf 2.5 Boeteverhogende en boeteverlagende omstandigheden

Artikel 8. Eventuele boeteverhoging of boeteverlaging

Indien naar het oordeel van de Autoriteit Persoonsgegevens sprake is van boeteverhogende of boeteverlagende omstandigheden, kan de boete, nadat toepassing is gegeven aan paragraaf 2.4, worden verhoogd dan wel verlaagd, vanwege omstandigheden als bedoeld in de artikelen 9 en 10. De Autoriteit Persoonsgegevens kan daarbij, met inachtneming van het wettelijk boetemaximum, buiten de grenzen van de boetebandbreedte treden.

Artikel 9. Boeteverhogende omstandigheden

9.1 De Autoriteit Persoonsgegevens merkt als boeteverhogende omstandigheden aan:
   a. de omstandigheid dat de Autoriteit Persoonsgegevens reeds eerder onherroepelijk een zelfde of een vergelijkbare door de overtreder begane overtreding heeft vastgesteld. In geval van recidive verhoogt de Autoriteit Persoonsgegevens de boete met 50%, tenzij dit gezien de omstandigheden van het concrete geval onredelijk zou zijn.
   b. de omstandigheid dat de overtreder het onderzoek van de Autoriteit Persoonsgegevens heeft tegengewerkt of belemmerd.

9.2 Niet-nakoming van een bindende aanwijzing, bedoeld in artikel 66, vijfde lid, van de Wet bescherming persoonsgegevens, wordt niet aangemerkt als hetzelfde type overtreding als de overtreding van de in artikel 66, tweede lid, van de Wet bescherming persoonsgegevens genoemde artikelen waarvoor de Autoriteit Persoonsgegevens de bindende aanwijzing heeft gegeven.

Artikel 10. Boeteverlagende omstandigheden

Boeteverlagende omstandigheden zijn in ieder geval:

a. de omstandigheid dat de overtreder verdergaande medewerking aan de Autoriteit Persoonsgegevens heeft verleend dan waartoe hij wettelijk gehouden was;
b. de omstandigheid dat de overtreder uit eigen beweging de overtreding heeft beëindigd voor of bij de eerste bekendwording met het onderzoek van de Autoriteit Persoonsgegevens;
c. de omstandigheid dat de overtreder uit eigen beweging degenen aan wie door de overtreding schade is berokkend, schadeloos heeft gesteld.

Paragraaf 2.6 Overige bepalingen met betrekking tot de oplegging van bestuurlijke boetes

Artikel 11. Meerdere overtredingen

Indien de Autoriteit Persoonsgegevens constateert dat een overtreder meerdere overtredingen heeft begaan, kan zij, in plaats van elke overtreding afzonderlijk te beboeten, een bestuurlijke boete opleggen voor deze overtredingen gezamenlijk.

Hoofdstuk 3. Slotbepalingen

Artikel 12. Intrekking oude beleidsregels

De Regels voor de boetevaststelling (*Stcrt.* 2003, nr. 123) worden ingetrokken.
De Beleidsregels CBP handhaving protocolplicht Wet politiegegevens (*Stcrt.* 2009, nr. 15761 en *Stcrt.* 2009, nr. 17372) en de bij dit besluit behorende bijlage worden ingetrokken.

Artikel 13. Inwerkingtreding

Deze beleidsregels treden in werking met ingang van de dag na de datum van uitgifte van de Staatscourant waarin ze worden geplaatst.

Artikel 14. Citeertitel

Deze beleidsregels worden aangehaald als: Boetebeleidsregels Autoriteit Persoonsgegevens 2015.

Artikel 15. Bekendmaking

Deze beleidsregels zullen met de toelichting in de Staatscourant worden geplaatst.

Den Haag, [*datum*]

Het College bescherming persoonsgegevens,

mr. J. Kohnstamm
Voorzitter

Bijlage 1, behorende bij artikel 2 van de Boetebeleidsregels Autoriteit Persoonsgegevens 2015

Overtredingen met een wettelijk boetemaximum van € 810.000

Wetsartikel	Omschrijving	Categorie
Wet bescherming persoonsgegevens		
artikel 6	behoorlijke en zorgvuldige gegevensverwerking	I, II of III
artikel 7	doeleindenomschrijving	II/III
artikel 8	grondslag gegevensverwerking	II/III
artikel 9, eerste lid	doelbinding	II/III
artikel 9, vierde lid	geen verwerking als geheimhoudingsplicht	II/III
artikel 10, eerste lid	maximale bewaartermijn	II
artikel 11, eerste lid	toereikende, ter zake dienende en niet bovenmatige gegevensverwerking	II
artikel 11, tweede lid	maatregelen opdat persoonsgegevens juist en nauwkeurig zijn	I/II
artikel 12, eerste lid	verwerking in opdracht verantwoordelijke	II
artikel 12, tweede lid	geheimhoudingsplicht bewerker	I/II
artikel 13	beveiligingsverplichting	II/III
artikel 16	verbod verwerking bijzondere persoonsgegevens	III
artikel 24, eerste lid	gebruik wettelijk identificatienummer	III
artikel 24, tweede lid	nadere regels gebruik wettelijk identificatienummer	II/III
artikel 33, eerste lid	informatieplicht persoonsgegevens verkregen bij betrokkene	II
artikel 33, tweede lid	te verstrekken informatie	II
artikel 33, derde lid	verstrekking nadere informatie	II
artikel 34, eerste lid	informatieplicht persoonsgegevens verkregen op andere wijze dan bij betrokkene	II
artikel 34, tweede lid	te verstrekken informatie	II
artikel 34, derde lid	verstrekking nadere informatie	II
artikel 34a, eerste lid	meldplicht datalekken bij Autoriteit Persoonsgegevens	II
artikel 34a, tweede lid	meldplicht aan betrokkene	II
artikel 34a, derde lid	inhoud kennisgeving	I
artikel 34a, vierde lid	inhoud kennisgeving aan Autoriteit Persoonsgegevens	I
artikel 34a, vijfde lid	wijze kennisgeving aan betrokkene	I
artikel 34a, zevende lid	alsnog verplichte kennisgeving aan	II

	betrokkene	
artikel 34a, achtste lid	bijhouden overzicht inbreuken	II
artikel 34a, elfde lid	nadere regels kennisgeving	I
artikel 35, eerste lid, tweede volzin	inzagerecht	II
artikel 35, tweede lid	inhoud mededeling	II
artikel 35, derde lid	zienswijze vragen derde	I
artikel 35, vierde lid	mededelingen logica geautomatiseerde verwerking	I
artikel 36, tweede lid	recht op verbetering, aanvulling, verwijdering of afscherming persoonsgegevens	II
artikel 36, derde lid	uitvoering beslissing op verzoek	II
artikel 36, vierde lid	informeren over onmogelijkheid van verbetering, aanvulling, verwijdering of afscherming	I
artikel 38, eerste lid	informeren derden over toewijzing verzoek	I
artikel 38, tweede lid	informeren verzoeker	I
artikel 39, eerste lid	maximale vergoeding inzageverzoek	I
artikel 39, tweede lid	teruggave vergoeding bij verbetering, aanvulling, verwijdering of afscherming	I
artikel 39, derde lid	gewijzigde maximale vergoeding	I
artikel 40, tweede lid	recht van verzet	II
artikel 40, derde lid	maximale vergoeding en teruggave vergoeding bij gegrond verzet	I
artikel 41, tweede lid	absoluut recht van verzet tegen verwerking voor commerciële of charitatieve doelen	II
artikel 41, derde lid	maatregelen om betrokkenen bekend te maken met recht van verzet	I
artikel 42, eerste lid	regels geautomatiseerde individuele besluiten	III
artikel 42, vierde lid	mededeling logica geautomatiseerde verwerking	I
artikel 66, vijfde lid	niet-nakoming bindende aanwijzing	I, II of III, afhankelijk van de indeling van het onderliggende artikel
artikel 76, eerste lid	verbod doorgifte naar land buiten EER zonder passend beschermingsniveau	II
artikel 77, tweede lid	voorschriften doorgiftevergunning	I
artikel 78, vierde lid	opschorting doorgifte bij ministeriële regeling of besluit	I

Algemene wet bestuursrecht		
artikel 5:20, eerste lid	medewerkingsplicht (nalevingstoezicht Wet bescherming persoonsgegevens)	I, II of III, afhankelijk van de indeling van het onderliggende artikel

Bijlage 2, behorende bij artikel 3 van de Boetebeleidsregels Autoriteit Persoonsgegevens 2015

Overtredingen met een wettelijk boetemaximum van € 450.000

Wetsartikel	Omschrijving	Categorie
Telecommunicatiewet		
artikel 11.3a, eerste lid	meldplicht datalekken aanbieder openbare elektronische communicatiedienst bij Autoriteit Persoonsgegevens	III
artikel 11.3a, tweede lid	meldplicht aan betrokkene	III
artikel 11.3a, derde lid	inhoud kennisgeving	II
artikel 11.3a, vierde lid	alsnog verplichte kennisgeving aan betrokkene	III
artikel 11.3a, zesde lid	bijhouden overzicht inbreuken	III
artikel 11.3a, zevende lid	nadere regels kennisgeving	II
Algemene wet bestuursrecht		
artikel 5:20, eerste lid	medewerkingsplicht (oplevering toezicht telecommunicatiewet)	II of III, afhankelijk van de indeling van het onderliggende artikel

Bijlage 3, behorende bij artikel 4 van de Boetebeleidsregels Autoriteit Persoonsgegevens 2015

Overtredingen met een wettelijk boetemaximum van € 20.250

Wetsartikel	Omschrijving	Categorie
Wet bescherming persoonsgegevens		
artikel 4, derde lid	aanwijzing vertegenwoordiger door verantwoordelijke buiten EER	II
artikel 78, tweede lid, aanhef en onder a	doorgifteverbod bij ministeriële regeling of besluit	II
Wet politiegegevens		
artikel 32, eerste lid	protocolplicht	II
artikel 32, tweede lid	melding gemeenschappelijke verwerking aan Autoriteit Persoonsgegevens	I
artikel 32, derde lid	bewaartermijn	II
artikel 32, vierde lid	nadere regels wijze vastlegging	I
Wet justitiële en strafvorderlijke gegevens		
artikel 19, eerste lid	vastlegging en bewaarplicht verstrekking justitiële gegevens	II
artikel 39j, eerste lid	vastlegging en bewaarplicht verstrekking strafvorderlijke gegevens	II
artikel 44, eerste lid	vastlegging en bewaarplicht verstrekking afschriften rapporten uit persoonsdossiers	II

TOELICHTING OP DE BELEIDSREGELS

Algemene toelichting

Uitbreiding boetebevoegdheid Autoriteit Persoonsgegevens

Op [*datum*] treedt de Wet meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid Cbp (Kamerstuknummers 33 662) in werking. Op grond van de Wet meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid Cbp kan de Autoriteit Persoonsgegevens een bestuurlijke boete (hierna: boete) opleggen ter zake van overtreding van onder andere alle hoofdverplichtingen van de verantwoordelijke uit de Wet bescherming persoonsgegevens (Wbp).

De bevoegdheid van de Autoriteit Persoonsgegevens om bij overtredingen van de Wbp een boete op te leggen, gold voorheen uitsluitend voor overtreding van artikel 27 en 28.

De keuze van de wetgever om over te gaan tot uitbreiding van de boetebevoegdheid is ingegeven door de wens de sanctiemogelijkheden van de Autoriteit Persoonsgegevens te versterken om de naleving van de Wbp, zowel door bedrijven als overheden, te bevorderen.[3] Met de uitbreiding van de boetebevoegdheid van de Autoriteit Persoonsgegevens wordt toegegroeid naar het handhavingssysteem uit de toekomstige Algemene verordening gegevensbescherming, die de Wbp als algemene wet zal gaan vervangen.[4] Ook het voorstel voor deze verordening voorziet in de bevoegdheid voor de nationale toezichthouders om boetes op te leggen bij overtreding van de verordening.

Boetebevoegdheid en wettelijk boetemaximum

De Autoriteit Persoonsgegevens is op grond van artikel 66 van de Wbp bevoegd een boete op te leggen ter zake van overtredingen van de in het eerste en tweede lid van dat artikel genoemde bepalingen van de Wbp, niet-nakoming van een bindende aanwijzing als bedoeld in artikel 66, vijfde lid, van de Wbp, en artikel 5:20 van de Algemene wet bestuursrecht (Awb) bij nalevingstoezicht op de Wbp.

De Autoriteit Persoonsgegevens kan voorts op grond van artikel 15.4, vierde lid, van de Telecommunicatiewet (hierna: Tw) een boete opleggen ter zake van overtredingen van de in artikel 15.1, derde lid, van deze wet bedoelde regels (de meldplicht voor datalekken in artikel 11.3a van de Tw), en artikel 5:20 van de Awb bij nalevingstoezicht op de Tw.

Tot slot kan de Autoriteit Persoonsgegevens op grond van artikel 35, derde lid, van de Wet politiegegevens (hierna: Wpg) en artikel 27, vierde lid, van de Wet justitiële en strafvorderlijke gegevens (hierna: Wjsg) een boete opleggen ter zake van overtredingen van een aantal bepalingen uit die wetten.

De beboetbare bepalingen uit de hiervoor genoemde wetten kennen een wettelijk boetemaximum van € 810.000, € 450.000 of € 20.250. Deze beboetbare bepalingen zijn, gegroepeerd per wettelijk boetemaximum, opgesomd en omschreven in bijlage 1 tot en met 3 bij deze beleidsregels.

[3] *Kamerstukken II* 2014/15, 33 662, nr. 9, p. 4.
[4] *Kamerstukken II* 2014/15, 33 662, nr. 9, p. 11.

Artikel 66, tweede lid, van de Wbp jo. artikel 23, zevende lid, van het Wetboek van Strafrecht biedt de Autoriteit Persoonsgegevens de mogelijkheid, indien de hoogste boetecategorie van € 810.000 geen passende bestraffing toelaat, aan een rechtspersoon een boete op te leggen tot ten hoogste tien procent van de jaaromzet van de rechtspersoon in het boekjaar voorafgaande aan het besluit waarbij de boete wordt opgelegd.

Bepalen van de hoogte van bestuurlijke boetes

Bij de vaststelling van (de hoogte van) de boete moet de Autoriteit Persoonsgegevens onder andere het wettelijk boetemaximum, de toepasselijke bepalingen van (hoofdstuk 5 van) de Awb en de algemene beginselen van behoorlijk bestuur in acht nemen.

De Autoriteit Persoonsgegevens kan omwille van de rechtsgelijkheid en rechtszekerheid beleid vaststellen en toepassen inzake de invulling van de bevoegdheid tot het opleggen van een boete, waaronder het bepalen van de hoogte daarvan. Met deze beleidsregels (hierna: Boetebeleidsregels) beoogt de Autoriteit Persoonsgegevens inzicht te geven in de factoren die de hoogte van de boete bepalen.

Artikel 4:84 van de Awb biedt de Autoriteit Persoonsgegevens de mogelijkheid van deze beleidsregels met betrekking tot het bepalen van de hoogte van boetes af te wijken vanwege bijzondere gevallen die niet in de beleidsregels zijn verdisconteerd (inherente afwijkingsbevoegdheid).

Drie jaar na inwerkingtreding van de Boetebeleidsregels worden deze geëvalueerd om te bezien of en in hoeverre de inhoud daarvan aanpassing behoeft. Te zijner tijd zal worden bekeken in welke vorm die evaluatie - waarbij externen zullen worden betrokken - zal plaatsvinden.

Bindende aanwijzing

Op grond van artikel 66, derde lid, van de Wbp moet de Autoriteit Persoonsgegevens eerst een bindende aanwijzing aan de overtreder geven, voordat zij kan overgaan tot het opleggen van een boete wegens overtreding van de in artikel 66, tweede lid, genoemde artikelen. De Autoriteit Persoonsgegevens kan de overtreder een termijn stellen waarbinnen de aanwijzing moet worden opgevolgd.

Deze verplichting een bindende aanwijzing te geven, alvorens een boete op te leggen, geldt niet indien de overtreding opzettelijk is gepleegd of het gevolg is van ernstig verwijtbare nalatigheid (zie het vierde lid van artikel 66 van de Wbp).

Bij de term 'opzettelijk gepleegd' valt volgens de wetsgeschiedenis te denken aan ongeoorloofde handel in persoonsgegevens. In dergelijke situaties gaat het bijvoorbeeld om overtreders die willens en wetens de regels overtreden om er zelf financieel beter van te worden.[5]

Onder 'het gevolg van ernstig verwijtbare nalatigheid' wordt volgens de wetsgeschiedenis verstaan: indien de overtreding het gevolg is van grof, aanzienlijk onzorgvuldig, onachtzaam dan wel onoordeelkundig handelen. Indien meerdere malen eenzelfde type overtreding heeft plaatsgevonden, kan sneller worden aangenomen dat sprake is van nalatigheid.[6]

[5] *Kamerstukken II* 2014/15, 33 662, nr. 9, p. 17.
[6] *Kamerstukken II* 2014/15, 33 662, nr. 16.

Systematiek Boetebeleidsregels: categorie-indeling en boetebandbreedtes

In deze Boetebeleidsregels is gekozen voor een categorie-indeling en bandbreedte systematiek.

De beboetbare bepalingen op de naleving waarvan de Autoriteit Persoonsgegevens toezicht houdt, zijn per wettelijk boetemaximum van € 810.000, € 450.000 of € 20.250 ingedeeld in een aantal boetecategorieën, en daaraan verbonden in zwaarte oplopende boetes.

De categorieën lopen op in zwaarte van de overtreding van de bepalingen, waarbij categorie I de minst zware overtredingen bevat en categorie II of III de zwaarste overtredingen.

Met de indeling in categorieën wordt, los van de concrete omstandigheden van de overtreding, een indicatie gegeven van de hoogte van de boete die wegens een bepaalde overtreding kan worden opgelegd.

Bij het bepalen van de categorie-indeling heeft de Autoriteit Persoonsgegevens zich georiënteerd op het concept voor de Algemene verordening gegevensbescherming. Ook het voorstel voor de verordening deelt de overtredingen in drie categorieën in, en verbindt daaraan in zwaarte oplopende bestuurlijke geldboetes.[7]

Bij de indeling van de bepalingen in de boetecategorieën heeft de Autoriteit Persoonsgegevens de zwaarte van de geschonden norm gewogen en beoordeeld. Het gaat daarbij om de waarde van de norm en zijn plaats in de hiërarchie van normen in het stelsel van privacy wet- en regelgeving, mede gelet op de daarmee te dienen doelen en de belangen die deze bepalingen beogen te beschermen. Daarnaast is bekeken in welke categorie de betreffende bepaling in het concept voor de Algemene verordening gegevensbescherming is ingedeeld.

Voor de algemene verplichtingen voor de verantwoordelijken uit hoofdstuk 2 van de Wbp met een wettelijk boetemaximum van € 810.000, geldt dat ze in beginsel nevengeschikt en niet ondergeschikt zijn ten opzichte van elkaar.[8] Dat betreft allereerst de hoofdverplichtingen uit de artikelen 6 tot en met 13. Die bepalingen betreffen de materiële normen die gelden voor alle verwerkingen van persoonsgegevens, waardoor, over het algemeen, de indeling in categorie II op zijn plaats is. Datzelfde geldt voor overtreding van de artikelen 33, 34 en 34a. Transparantie is eveneens een hoofdverplichting van de verantwoordelijke.[9] Ten aanzien van de meldplicht voor datalekken heeft de Autoriteit Persoonsgegevens zich georiënteerd op de beleidsregel die door de Minister van Economische Zaken is vastgesteld voor het opleggen van bestuurlijke boetes door de Autoriteit Consument en Markt ter zake van overtreding van de meldplicht voor datalekken in artikel 11.3a van de Tw (Boetebeleidsregel ACM 2014).[10]

Ook voor de rechten van de betrokkene in hoofdstuk 6 geldt dat ze in beginsel nevengeschikt en niet ondergeschikt zijn ten opzichte van elkaar.[11] Dit betreft de overtredingen van de artikelen 35 tot en met 42 van de Wbp. Bij het bepalen van de categorie-indeling is er vanuit gegaan dat de

[7] De maximale boete in het voorstel is 1 miljoen euro of, voor een onderneming, 2% van de jaarlijkse wereldwijde omzet (artikel 79 van het concept Algemene verordening gegevensbescherming).
[8] *Kamerstukken II* 2014/15, 33 662, nr. 9, p. 19.
[9] Zie ook *Kamerstukken II* 2014/15, 33 662, nr. 9, p. 17-18.
[10] Vgl. *Kamerstukken II* 2014/15, 33 662, nr. 9, p. 19-20.
[11] *Kamerstukken II* 2014/15, 33 662, nr. 9, p. 19.

verplichtingen die de verantwoordelijken hebben bij de behandeling van verzoeken van betrokkenen om inzage, correctie en verzet in belangrijke mate van juridisch-administratieve aard zijn.[12] De materiële rechten van de betrokkene zijn ingedeeld in categorie II. De bepalingen die meer procedurele waarborgen bieden, zoals artikel 35, derde lid, van de Wbp, zijn ingedeeld in categorie I. Hetzelfde geldt in grote lijnen voor de verplichtingen die voortvloeien uit de regeling van de doorgifte van persoonsgegevens naar landen buiten de Europese Economische Ruimte zonder een passend beschermingsniveau. Dit betreft de overtredingen van de artikelen 76 tot en met 78 van de Wbp.[13]

De indeling in categorie III heeft te maken met de aard van het geschonden rechtsgoed, zoals het voorkomen van misbruik van de verwerking van gevoelige informatie over personen en het daaruit voortvloeiende kennispotentieel met betrekking tot andere personen[14] dan wel de bescherming van de menselijke waardigheid. Artikel 16 van de Wbp bevat het belangrijke verbod op het verwerken van bijzondere persoonsgegevens. Overtreding van artikel 24 van de Wbp kan aan de orde zijn bij het buitenwettelijk gebruik van persoonsidentificerende nummers. Artikel 42 van de Wbp beschermt tegen besluitvorming ten aanzien van enige natuurlijke persoon op grond van een profielschets of een persoonlijkheidsschets die langs geautomatiseerde weg tot stand is gebracht. Uit de wetsgeschiedenis kan worden opgemaakt dat de menselijke waardigheid vereist dat dergelijke beslissingen over iemand door een andere persoon, en niet slechts door een geautomatiseerd systeem, worden genomen.[15]

Elke boetecategorie is gekoppeld aan een bepaalde boetebandbreedte die de Autoriteit Persoonsgegevens passend en geboden voorkomt. Dit betekent dat de hoogte van de boete evenredig moet zijn en voldoende afschrikwekkend voor zowel de overtreder (speciale preventie) als andere potentiële overtreders (generale preventie). Binnen deze bandbreedte stelt de Autoriteit Persoonsgegevens een basisboete vast.

De hoogte van de boete stemt de Autoriteit Persoonsgegevens in ieder geval af op de factoren die zijn genoemd in artikel 6. Het gaat daarbij om de ernst van de concrete overtreding, de mate waarin de overtreding aan de overtreder kan worden verweten en, indien daar aanleiding toe bestaat, andere omstandigheden, zoals de (financiële) omstandigheden waarin de overtreder verkeert (zie artikel 5:46 van de Awb). Bij de bepaling van de uiteindelijke hoogte van de boete houdt de Autoriteit Persoonsgegevens voorts rekening met de aanwezigheid van boeteverhogende en boeteverlagende factoren als bedoeld in de artikelen 9 en 10 om bijzondere omstandigheden met betrekking tot de overtreder mee te kunnen wegen. De Autoriteit Persoonsgegevens kan daarbij, zo nodig, buiten de grenzen van de boetebandbreedte treden. Een boeteverhogende factor kan uiteraard niet leiden tot een boete die boven het wettelijk boetemaximum uitstijgt.

[12] Zie ook *Kamerstukken II* 2014/15, 33 662, nr. 9, p. 17-18.
[13] *Kamerstukken II* 2014/15, 33 662, nr. 9, p. 18.
[14] Dat raakt aan het verbod op het maken van onderscheid tussen personen op grond van godsdienst, levensovertuiging, politieke gezindheid, ras, geslacht etc. (o.a. artikel 1 van de Grondwet). Vgl. *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 11 en *Kamerstukken II* 2014/15, 33 662, nr. 9, p. 11.
[15] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 170.

Artikelsgewijze toelichting

Artikel 6, eerste lid

De Autoriteit Persoonsgegevens stemt de beoordeling van de aard en omvang van de overtreding in ieder geval af op: de schaal waarop de overtreding heeft plaatsgevonden, de intensiteit van de overtreding en het stelselmatige of incidentele karakter ervan.

De Autoriteit Persoonsgegevens stemt de beoordeling van de impact van de overtreding op (de bescherming van persoonsgegevens en van de persoonlijke levenssfeer voor) de betrokkenen en/of de maatschappij bijvoorbeeld af op: het (financiële) voordeel dat de overtreder heeft behaald met de overtreding en/of de schade die betrokkenen hebben geleden door de overtreding.

Artikel 6, tweede lid, tweede volzin

De tweede volzin van dit artikellid maakt duidelijk dat het criterium 'opzettelijk of ernstig verwijtbaar nalatig handelen' in artikel 66, vierde lid, van de Wbp een aanzienlijke mate van verwijtbaarheid veronderstelt. Dat heeft, in gevallen waarin de Autoriteit Persoonsgegevens een boete oplegt aan de overtreder zonder eerst een bindende aanwijzing te geven, bij de vaststelling van de hoogte van de boete overeenkomstig paragraaf 2.4 gevolgen voor de beoordeling van de mate waarin de overtreding aan de overtreder kan worden verweten.

Artikel 7, eerste lid

De Autoriteit Persoonsgegevens kan de boetebandbreedte van de naast hogere categorie respectievelijk de bandbreedte van de naast lagere categorie toepassen indien de hoogte van de boete, gezien de omstandigheden van het geval, anders niet voldoende preventieve werking heeft dan wel onevenredig hoog is.

Artikel 7, tweede lid

Indien in voorkomende gevallen een boete van € 810.000 geen passende bestraffing toelaat, kan de Autoriteit Persoonsgegevens een boete opleggen tot ten hoogste tien procent van de jaaromzet van een rechtspersoon. Op voorhand is niet vast te stellen in welke gevallen daarvan sprake zal zijn. De hoogte van de boete zal worden bepaald aan de hand van de relevante factoren die opgesomd staan in artikel 6 van de Boetebeleidsregels en dient in een concreet geval overeenkomstig artikel 3:46 van de Algemene wet bestuursrecht deugdelijk gemotiveerd te worden.

Artikel 8

Indien in een concreet geval sprake is van boeteverlagende (of -verhogende) omstandigheden kan, na het bepalen van de boeteverlaging (of -verhoging), buiten de bandbreedte (en de voor de overtreding bepaalde boetecategorie) worden getreden.

Artikel 9, eerste lid

Een boeteverhoging vanwege de omstandigheid dat de overtreder het onderzoek van de Autoriteit Persoonsgegevens heeft tegengewerkt of belemmerd, is mogelijk voor zover dit geen

afbreuk doet aan de rechten van verdediging die een overtreder toekomen. Een dergelijke boeteverhoging is niet mogelijk indien een boete aan de overtreder is of wordt opgelegd wegens niet-meewerken aan het onderzoek (artikel 5:20 van de Awb).

Artikel 9, tweede lid

Dit artikel maakt duidelijk dat de enkele niet-nakoming van een bindende aanwijzing als bedoeld in artikel 66, vijfde lid, van de Wbp nog geen recidive veronderstelt, omdat geen sprake is van hetzelfde type overtreding van het onderliggende artikel in de zin van dit tweede lid. Dat is ook van belang omdat de ratio van de regeling van de bindende aanwijzing is dat de Autoriteit Persoonsgegevens in de bindende aanwijzing ter concretisering van de wettelijke norm moet aangeven welke gedraging op grond van de Wbp van de verantwoordelijke wordt verwacht. Dit houdt verband met het algemeen-abstracte karakter van de normen van de Wbp en het lex certa-beginsel.[16] Onduidelijkheid over de invulling van de betreffende norm behoort dan ook geen boeteverhogende factor te zijn.

Artikel 10

Bij het criterium 'verdergaande medewerking verleend aan de Autoriteit Persoonsgegevens dan waartoe de overtreder wettelijk gehouden was', bedoeld in artikel 10, onder a, valt te denken aan de situatie waarin de overtreder niet alleen medewerking aan het onderzoek heeft verleend (bijvoorbeeld een verklaring heeft willen afleggen), maar ook sprake is van een daadwerkelijk verdergaande medewerking aan het onderzoek dan waartoe de overtreder wettelijk was gehouden.

Het criterium dat 'de overtreder de overtreding heeft beëindigd voor of bij de eerste bekendwording met het onderzoek van de Autoriteit Persoonsgegevens' heeft betrekking op gevallen waarin de overtreder heeft gehandeld met het oogmerk om actief (uit eigen beweging) de overtreding te beëindigen.

[16] *Kamerstukken II* 2014/15, 33 662, nr. 9, p. 4.

Bijlage 5. Audit WML

Memo

Aan Het managementteam WML
Van Wilma Hermans en Conny Kleijssen
Betreft Managementrapportage n.a.v. gehouden audit werkplekken in het kader van de Wet bescherming persoonsgegevens en richtlijnen zoals opgenomen in het privacyreglement van WML
Datum 15 juni 2009
==========

Geacht management,

Hierbij doen wij u ter informatie een rapportage toekomen van de op 26 mei 2009 vanaf 16.45 uur voor de **4de keer** gehouden audit inzake het uitvoering geven aan de Wet Bescherming persoonsgegevens en hiermee aan het door WML opgestelde beleid "privacyreglement personeelsregistratie WML". Hiertoe is steekproefsgewijs een aantal werkplekken in de organisatie onderzocht en is gekeken of daar persoonsgegevens (dit zijn alle gegevens die herleidbaar zijn naar een identificeerbare persoon) "onbeveiligd" oftewel in een niet afgesloten kast of bureaulade c.q. rolcontainer, en daardoor toegankelijk voor een ieder, te vinden waren. De constateringen worden hierbij op naam, van diegenen waarvan de werkplek in het kader van deze audit is onderzocht, vertrouwelijk teruggerapporteerd.

Divisie Industrie

Kantoor industriële detachering (gebouw 2):
Werkplek J. Boons (audit 4de x)
Deze werkplek is voor de 4de keer onderworpen aan de audit, omdat deze keer op keer als zwaar onvoldoende scoort. De werkplek voldeed bij de 1ste, 2de en 3de audit niet aan de gestelde eisen en ook bij de 4de audit voldoet deze werkplek opnieuw niet. Is duidelijk een punt van aandacht! Kasten, bureaulades/rolcontainers waren open. Hierin bevonden zich o.a. portfolio's van medewerkers, ziektegegevens van medewerkers, loonstroken van medewerkers, coachingsplannen van collega's, brieven disciplinaire maatregelen aan medewerkers, personeelslijsten etc. Geen clean desk!

Werkplek D. Paf (audit 1ste x)
Op het bureau wordt een brief aangetroffen over aanpassing dienstverband van een medewerker. Geen clean desk! Rolcontainer niet op slot maar geen P-gegevens.

Werkplek J. Krijnen (audit 1ste x)
Op het bureau liggen P-gegevens o.a. weekstaten medewerkers, agenda's met namen data en afspraken. Geen clean desk! Rolcontainer is niet op slot en ook daarin zitten portfolio's van medewerkers.

Conclusie kantoor industriële detachering: dit kantoor krijgt een zware onvoldoende m.b.t. de bescherming van P-gegevens en is zeker een punt van aandacht. Overal zitten sleutels op en niets is afgesloten! Alles is voor iedereen toegankelijk terwijl hier nadrukkelijk met P-gegevens wordt gewerkt.

Kantoor Cleanroom (gebouw 2):
Werkplek W. van Son (audit 1ste x)
Kast en bureaulade niet afgesloten maar geen P-gegevens aanwezig, dus is prima. Wel ligt op het bureau een mutatieoverzicht uit Axapta met n.a.w. gegevens.

Werkplek E. van Beek (audit 1ste x)

Geen P-gegevens aangetroffen dus prima, wel zijn in de kasten van cleanroom klantgegevens aanwezig.

Werkplek H. Kuipers (audit 3de x)
Ook deze werkplek is, omdat deze de vorige twee keren onvoldoende scoorde, opnieuw onderworpen aan de audit. Het kantoor was afgesloten na werktijd en je kunt je afvragen of dat de bedoeling is. Kast was op slot maar rolcontainer was open en hierin lagen P-gegevens. Er lag van alles op het bureau. In ieder geval geen clean desk! Punt van aandacht blijft ondanks dat er in vergelijking met vorige keren wel verbetering is opgetreden. Vraag blijft of het kantoor na werktijd moet zijn afgesloten of dat gewoon de kast en rolcontainer op slot worden gedaan? In het kader van de algehele veiligheid lijkt ons het laatste het geval.

Divisie Diensten

Werkplekken N. Sprangers, R. de Jong (audit 3de x)
In z'n algemeenheid moet worden opgemerkt dat in vergelijking met vorige keren de verzorging van de werkplekken is verbeterd al is er nog steeds geen sprake van een clean desk! Wel blijft nadrukkelijk punt van aandacht, zoals ook de vorige keren is geconstateerd, dat alle sleutels van voertuigen en externe objecten open en bloot op de bureaus liggen en in het sleutelkastje hangen met aan deze sleutels de namen van voertuigen en objecten, kortom deze kunnen zomaar door iedereen worden meegenomen! Verder liggen mobiele telefoons op bureaus en kunnen ook zomaar worden meegenomen! Geen P-gegevens aangetroffen dus is prima, bepaalde kasten zijn afgesloten andere zijn open maar geen P-gegevens. Rolcontainers open maar geen P-gegevens. Wel overal klantgegevens te vinden.

Werkplekken P. Frodyma en M. van Laarhoven (audit 2de x)
Op deze werkplekken was niets afgesloten, geen kasten en geen rolcontainers, zelfs kasten stonden volledig open. Verder geen P-gegevens aangetroffen wel overal klantgegevens. Kortom, geen P-gegevens is prima echter nog wel aandacht voor afsluiten kasten en rolcontainers en clean desk!

Werkplek A. Peters (audit 2de x)
Deze werkplek voldeed aan de gestelde richtlijnen. Het was een clean desk, de kast was op slot, de rolcontainer was afgesloten, kortom, geen enkele informatie of gegevens over personen en medewerkers te vinden. Prima werkplek!

Kantoor administratie re-integratie:
Werkplek E. van Unen (audit 3de x)
De kasten op het kantoor van re-integratie zijn afgesloten en ook in het postvakje bevinden zich geen P-gegevens, kortom prima. Echter, de werkplek van E. van Unen is de rolcontainer opnieuw open (ook vorige twee keren het geval) en daarin bevinden zich een groot aantal P-gegevens. Kortom, werkplek voldoet voor de 3de keer niet aan gestelde eisen! Nadrukkelijk punt van aandacht, zeker omdat hier alleen maar met P-gegevens wordt gewerkt!

Werkplek J. van Hoof (audit 4de x)
Werkplek voldoet aan de gestelde richtlijnen, er is sprake van clean desk, kast en rolcontainer zijn op slot en in vergelijking met vorige keer verbetering m.b.t. het postvakje, ook hierin nl. geen P-gegevens aanwezig. Prima werkplek!

Kantoor intercedenten re-integratie:
Werkplek M. Tannemaat (audit 4de x)
Omdat deze werkplek de 3 eerdere keren niet voldeed aan de richtlijnen is deze opnieuw onderworpen aan de audit en ook opnieuw voldoet deze werkplek niet. Kortom, zeer nadrukkelijk punt van aandacht, mede omdat hier enkel met P-gegevens wordt gewerkt. Er is geen sprake van clean desk, de rolcontainer is niet op slot en hierin bevinden zich o.a. trajectgegevens van cliënten. Verder zit het doosje "oud papier" dat voor het bureau staat vol met P-gegevens!

Werkplek S. Hamers (audit 1ste x)
De rolcontainer is niet afgesloten, maar ook geen P-gegevens aanwezig, verder cleandesk dus werkplek voldoet.
Werkplek M. de Bont (audit 2de x)

De rolcontainer is afgesloten, sprake van cleandesk alleen de kast (in het midden van het kantoor) is niet afgesloten en deze zit vol met mappen met P-gegevens! Punt van aandacht is dus de kast!

Werkplek J. Kirsch (audit 1ste x)
De rolcontainer is niet afgesloten en zit vol met P-gegevens! Punt van aandacht!

Werkplek B. Flipsen (audit 1ste x)
Rolcontainer op slot alleen op het bureau lijst met opdrachten van re-integratie met daarop namen, BSN-nummers e.d. van cliënten. Punt van aandacht!

Werkplek I. Klomp (audit 2de x)
Rolcontainer op slot, cleandesk, enkel een ordner aanwezig met P-gegevens en algemene info over cliënten. Jammer, werkplek zag er verder o.k. uit!

Werkplek D. Melissen (audit 2de x)
Rolcontainer op slot, cleandesk, werkplek prima.

Stafafdelingen

Werkplek J. Hesselmans (audit 1ste x)
Kasten zijn afgesloten, rolcontainer is afgesloten, echter het bureau is het rommelig (geen cleandesk) maar geen P-gegevens aanwezig. Er wordt wel een ordner op het bureau aangetroffen met ziekteverzuimgegevens van medewerkers. Punt van aandacht is het bureau! Volgen van clean desk policy!

Werkplek I. van Opbergen (audit 3de x)
I.t.t. de twee eerdere keren is deze werkplek nu prima in orde. Rolcontainers en kasten zijn afgesloten en er is sprake van een clean desk.

Werkplek M. van Hulten (audit 3de x)
Ook de 3de keer, net als de vorige keren, is deze werkplek niet in orde. De rolcontainers zijn niet afgesloten en hierin bevinden zich veel P-gegevens. Bovendien is het bureau erg rommelig en ook daar overal P-gegevens te vinden, kortom zeker geen clean desk. Deze werkplek is punt van aandacht mede omdat hier veelal met P-gegevens wordt gewerkt.

Werkplek H. Giezenberg (audit 3de x)
Eén rolcontainer is afgesloten en één rolcontainer niet en hierin bevinden zich o.a. gegevens van het PAF over medewerkers. Overigens was dit de eerste 2 keren ook het geval en komt hier dus geen verandering in. Op het bureau is sprake van een clean desk. Punt van aandacht blijven de PAF-gegevens. Kortom, de werkplek is redelijk op orde.

Werkplek C. Huiben (audit 3de x)
De rolcontainers zijn niet afgesloten en hierin bevinden zich P-gegevens, o.a. verzoeken van OPJ m.b.t. medewerkers en klantgegevens. Wel is er sprake van een clean desk. Punt van aandacht is het sluiten van de rolcontainers.

Werkplek A. Speijers (audit 1ste x)
Eén rolcontainer is afgesloten en één niet en daarin bevinden zich P-gegevens zoals o.a. pensioen- en adresgegevens. Verder is er wel sprake van een clean desk. Aandachtspunt is de niet afgesloten rolcontainer.

Naar aanleiding van de uitgevoerde audit 2009 wordt het volgende aan het MT voorgesteld:

1. Nogmaals in de diverse werkoverleggen met de leidinggevenden opnieuw voor dit onderwerp in z'n algemeenheid aandacht (blijven) vragen. Bescherming van P-gegevens is nu eenmaal een belangrijk onderwerp, niet alleen voor medewerkers maar ook voor externe klanten;
2. notoire overtreders (rood gemarkeerd), dus diegenen waarvan de werkplek voor een 3de of 4de keer als onvoldoende wordt beoordeeld hierop nadrukkelijk aanspreken (en wellicht schriftelijk bevestigen) door de leidinggevende. Vooral speelt dit bij zogenoemde "kwetsbare functies" oftewel functies waarbij veelal of alleen maar met persoons-, c.q. medewerkersgegevens wordt gewerkt en waarbij het zorgvuldig en integer omgaan met persoonsgegevens een kerncompetentie moet zijn waarover de functionaris moet beschikken. Ook zou dit door de

leidinggevende meegenomen kunnen worden in het item “zorg materiaal/werkplek” zoals dit op het huidig beoordelingsformulier staat vermeld;

3. kijkend naar de rommelige bureaus van veel werkplekken nadrukkelijk aandacht blijven vragen voor de “clean desk policy” binnen WML;
4. benadrukken dat in het kader van de algehele veiligheid en het feit dat bijv. de beveiliging alsnog overal in kan, het niet de bedoeling is dat kantoren na werktijd worden afgesloten om hierdoor te omzeilen dat P-gegevens niet afgesloten opgeborgen hoeven te worden;
5. ten slotte vragen wij ons af of het houden van audits in dit kader toegevoegde waarde heeft en serieus wordt genomen, omdat het omgaan met P-gegevens in de organisatie zeker nog niet voldoende is en er slechts bij bepaalde werkplekken verbetering is opgetreden, ondanks dat we hier reeds vanaf 2006 nadrukkelijk aandacht voor vragen en op deze manier mee omgaan.

Bijlage 6. De zeven principes van privacy by design[1]

1. *Voorkomen is beter dan genezen*
   Privacy by design zorgt ervoor dat privacy risico's zo klein mogelijk blijven, door vooraf al over deze risico's na te denken en maatregelen te treffen. Het voorkomen van privacy inbreuken staat centraal.

2. *Privacy is de standaard*
   Producten en diensten moeten standaard ingesteld zijn om de hoogste mate van privacy te bieden. In dat geval is privacy als het ware ingebouwd in de systemen (dit principe wordt privacy by default genoemd).

3. *Integreren van gegevensbescherming en beveiliging in het ontwerp*
   Privacy by design zorgt ervoor dat privacy een kerncomponent wordt van je producten of diensten. Tijdens de ontwikkeling wordt privacy een integraal onderdeel van het product of dienst, zonder afbreuk te doen aan de functionaliteit daarvan.

4. *Volledige functionaliteit*
   Het is van groot belang dat privacy niet ten kosten gaat van bijvoorbeeld beveiliging. Door privacy in de ontwikkelingsfase in te bouwen in de systemen hoef je geen afweging te maken tussen beveiliging en privacy of tussen privacy en andere functionaliteiten.

5. *End-to-end beveiliging - Bescherming gedurende de hele levenscyclus*
   Privacy by design houdt rekening met privacy gedurende de gehele levenscyclus van de persoonsgegevens. Dit betekent dat alle persoonsgegevens veilig opgeslagen worden en ook op een juiste manier worden vernietigd.

6. *Zichtbaarheid en transparantie*
   Privacy by design staat voor openheid en transparantie. Deze transparantie creëert vertrouwen bij alle betrokken partijen. Klanten en leveranciers kunnen zien dat je privacy serieus neemt en je geeft openheid over hoe er met persoonsgegevens wordt omgegaan in de organisatie.

7. *Respect voor privacy van de betrokkene – de betrokkene staat centraal*
   Wellicht het belangrijkste aspect van privacy by design is dat de gebruiker of klant centraal staat. De belangen van de betrokkenen staan altijd op de eerste plek door het aanbieden van sterke standaard instellingen, transparantie, duidelijke communicatie en gebruiksvriendelijke mogelijkheden.

Privacy by design betekent dus niet alleen het inbouwen van privacy in systemen zelf, maar ook in werkprocessen, de managementstructuur en het bovenliggende netwerk.

[1] 'De zeven principes van privacy by design', I. Smittenberg, www.privacycompany.eu (zoek op *privacy by design*).

Bijlage 7. Interview coördinator van de afdeling personeelsadministratie
Het interview met de coördinator van de afdeling personeelsadministratie is in deze bijlage uitgetypt. Haar antwoorden zijn verwerkt in het onderzoeksrapport.

1. **Welke persoonsgegevens van sw-medewerkers worden verwerkt?**
   Onderscheid algemene persoonsgegevens en bijzondere persoonsgegevens.

Ik muteer het meest en dan muteer ik zowel algemene persoonsgegevens als bijzondere gegevens. Denk hierbij aan:
- Naam, adres, woonplaats
- BSN
- Medische gegevens.

Medische gegevens zijn bij de bedrijfsarts en de deze zet bijna nooit medische gegevens in rapporten. Wanneer een sw-medewerker een indicatie kreeg, stond er vaak wat de medewerker aan zijn gezondheid had om te kunnen komen werken bij Baanbrekers. Deze informatie werd in Compas gevoerd, maar in codes. Herindicatie van een medewerker wordt in het fysieke dossier gedaan.

2. **Hoe worden de persoonsgegevens verzameld?**

- *Wordt het aan de medewerkers gevraagd?*
- *Tijdens overleg? Mondeling, schriftelijk via bijvoorbeeld een formulier of digitaal?*
- *Worden de gegevens van andere organisaties overgenomen?*
- *Zijn de gegevens afkomstig van de gemeentes?*

Alles wordt op formulier gedaan. Mensen die nog een herindicatie hadden, kwamen binnen met medische gegevens en werden op een wachtlijst geplaatst. Er werden setjes gemaakt van formulieren voor deze medewerkers, die bij het aannameprocedure volledig ingevuld moesten worden. Deze formulieren werden in de fysieke dossiers gedaan en bevinden zich nog steeds in deze dossiers.

Daarnaast wordt de afdeling personeelsadministratie bediend door afdeling P&O. Stel dus dat een medewerker van een soortgelijke organisatie wordt overgenomen uit Nijmegen omdat hij bijvoorbeeld in gemeente Heusden, Waalwijk of Loon op Zand is gaan wonen, dan neemt de afdeling P&O van die organisatie contact op met de afdeling P&O van Baanbrekers. Zij kunnen de informatie betreffende de sw-medewerker fysiek of digitaal opsturen. Via de afdeling P&O komt het terecht bij de afdeling personeelsadministratie.

3. **Wordt vanuit afdeling P&O ook toezicht gehouden op de juiste verwerking van persoonsgegevens?**

Ik ben zelf de coördinator van de afdeling personeelsadministratie. Ik houd mij bezig met de dagelijkse leiding op de afdeling. Mijn taak is het verdelen van werk en verantwoordelijk zijn voor de export. Ik zorg ervoor dat gestelde procedures worden opgevolgd en ik hou controle op hoe mijn collega's muteren. Ik ben diegene die de laatste controle doet en uiteindelijk onderteken. Daarnaast wordt de afdeling personeelsadministratie gecontroleerd door de afdeling P&O en de afdeling interne beheersing.

4. **Gegevens die de afdeling direct van medewerkers krijgt door middel van bijvoorbeeld ingevulde formulieren, worden die meteen digitaal gezet en ook in dossiers?**

Alles gaat nog steeds in de fysieke dossiers. Ook van de brieven die worden aangemaakt in Compas, worden de aangetekende versies in de fysieke dossiers gedaan. In Compas kan namelijk nog niet digitaal getekend worden. Een kopie van alles kan gescand worden en in Compas worden geplaatst. Er zijn echter nog veel documenten die zich bevinden in de papieren dossiers.

5. **Op grond van welk (privacy) beleid of bijzondere wetgeving verwerken jullie persoonsgegevens?**

Er wordt op de afdeling niet aan de hand van een beleid gewerkt. Zelf weten wij ook niet van het bestaan van een privacybeleid binnen Baanbrekers. Alhoewel ik er wel zeker van ben dat wij deze onbewust zo veel mogelijk naleven.

6. **Welke handelingen van gegevensverwerking verrichten jullie voornamelijk?**

Aan de hand van de autorisatie die een werknemer van de afdeling personeelsadministratie krijgt, wordt bepaald welke handelingen van gegevensverwerking deze kan verrichten. Alle handelingen die genoemd zijn in artikel 1 lid b Wbp kunnen door ons worden verricht. Het enige wat ik als coördinator kan doen ten opzichte van de andere medewerkers van de afdeling is het verwijderen van persoonsgegevens. De afdeling personeelsadministratie is wel één van de afdelingen die alles kan zien en het meest kan doen met de persoonsgegevens.

7. **Welke gegevens kunnen tot nu toe niet benut worden in Compas**

Er is geen gegeven die ik op het moment specifiek kan opnoemen. Ik weet dat wij bij overname alleen gegevens kunnen muteren als deze via een aannameformulier bij ons op de afdeling worden aangeleverd.

8. **Hoe worden medische dossier gecodeerd in Compas?**

Wat betreft de gezondheid van een sw-medewerker staan, zoals bij vraag 1 is geantwoord, geen specifieke medische gegevens in. Wel zijn verbeterpunten en analyses opgenomen in Compas. Medische gegevens worden als volgt gecodeerd: in plaats van te zeggen wat de sw-medewerker heeft, wordt geadviseerd welke werkzaamheden de medewerker wel of niet kan verrichten.

9. **Hoe worden persoonsgegevens extern verwisseld?**

De medewerkers van de afdeling P&O moeten aan de medewerkers van de afdeling personeelsadministratie aangeven welke persoonsgegevens extern uitgewisseld moeten worden. Uitwisseling van persoonsgegevens wordt vooral gedaan bij herindicatie. Indien het een rapport is, dat niet toegankelijk is voor alle personen, dan gaat het document in een envelop waarop bijvoorbeeld staat: “vertrouwelijk en dient alleen geopend te worden door.. adviseur.”

10. **Met welke externe organisaties word informatie verwisseld?**

Extern wordt niet veel verstuurd. NAW-gegevens worden uitgewissel, maar BSN niet. Zelfs intern wordt bijna niets met BSN gestuurd. Digitaal niet en per post niet. Externe organisaties kunnen medische gegevens verkrijgen van de bedrijfsarts.

Ik zorg als coördinator wel erg op het voorkomen van een datalek. Alhoewel ik geen beleid heb of reglement die ik navolg, probeer ik wel zorgvuldig om te gaan met de persoonsgegevens. Ik zorg ervoor dat niets wat de persoon zou kunnen schaden de deur uitgaat.

11. **Hoe werken jullie toe naar de Algemene Verordening Gegevensbescherming?**

De afdeling personeelsadministratie heeft zich voorbereid op alle wijzigingen door het archief te ordenen. Twee jaar geleden moest alles worden geordend. De normen van de Archiefwet zijn aangepast en binnen Baanbrekers is besloten de dossiers tien jaar te bewaren. Toezicht op de naleving wordt, vanaf twee jaar geleden, elk jaar gehouden door de gemeenten.

Als een medewerker uit dienst gaat, is de laatste brief die de medewerker van Baanbrekers ontvangt bepalend voor de datum van vernietiging.

Bijlage 8. Interview systeembeheerder van Compas
Het interview met de systeembeheerder is in deze bijlage uitgetypt. Zijn antwoorden zijn verwerkt in het onderzoeksrapport.

1. **Hoe lang wordt bij Baanbrekers al gebruik gemaakt van Compas?**
   Baanbrekers werd al gebruikt bij WML. Sinds het bestaan van Baanbrekers, in 2013, is gebruik gemaakt van Compas binnen Baanbrekers.

2. **Welke persoonsgegevens kunnen in Compas worden ingevoerd?**
   Zowel algemene als bijzonere persoonsgegevens kunnen in Compas worden ingevoerd. Voorbeeld van de gegevens die ingevoerd kunnen worden, zijn: BSN, geboortedatum, geboorteplaats, geslacht.

3. **Wie is bevoegd om in Compas te kijken?**
   Niet alle reguliere medewerkers hebben toegang tot Compas. De autorisatie die voor het systeem verkregen moet worden, is functiegericht. Medewerkers van afdeling re-integratie en participatie en afdeling inkomensondersteuning hebben bijvoorbeeld geen toegang tot Compas. maar met verschillende autorisatie profielen. Deze medewerkers kunnen in Compas raadplegen, notities maken en brieven maken voor de sw-medewerkers. Elk adviseur kan in de dossiers van haar cliënten, maar ook de cliënten van haar collega. Dit is voor de gevallen waarbij de adviseurs elkaar zouden moeten vervangen. Medewerkers van de afdeling personeelsadministratie zijn de enige medewerkers die in Compas kunnen muteren.

   De leidinggevende van de afdeling P&O heeft toegang tot de gegevens van alle medewerkers die onder de afdeling vallen.

4. **Wat moet gebeuren voordat een werknemer in Compas kan?**
   Om te beginnen moet de autorisatieformulier door de manager van de organisatieonderdeel getekend moet worden. Op dat formulier wordt aangeven wat een reguliere medewerker nodig heeft voor de uitoefening van haar of zijn functie.
   Denk hierbij aan een werkplek, pc, toegang tot het netwerk en applicaties. Één van de complicaties is Compas. Dit formulier dient daarna terecht te komen bij de systeembeheerder. De systeembeheer controleert of er een geheimhoudingsverklaring is. Daarna bepaalt hij aan de hand van het autorisatieformulier welke bevoegdheden de medewerker krijgt in Compas. Via de afdeling krijgt een medewerker toegang tot het netwerk en daarna zorgt de systeembeheerder ervoor dat de medewerker toegang krijgt tot Compas.

5. **Hoe wordt ervoor gezorgd dat bevoegden alleen bij relevante gegevens terecht kunnen?**
   Dit wordt door de systeembeheerder gewaarborgd door een medewerker per functie, per persoon, per gegeven toegang te geven in Compas.
   Het kan voorkomen dat een medewerker die normaliter geen toegang heeft tijdelijk toegang krijgt voor het uitvoeren van een project. Na het project wordt de medewerker weer uitgesloten van toegang.

6. **Wat houden jouw taken als systeembeheer zijnde in?**

Ik zorg ervoor dat Compas constant wordt bijgewerkt naar de nieuwste versie. Ik richt ook het systeem in. Nieuwe organisatiestructuren of afdelingen zet ik erin, zodat de medewerkers van de afdeling personeelsadministratie erin kunnen muteren. Verder voer ik zaken met betrekking tot de helpdesk uit. Tot slot bepaal ik welke gegevens wel en niet geëxporteerd kunnen worden. Dus kortom voer ik zaken uit van systeemniveau, die worden gebruikt door een verschillende afdelingen.

7. **Wie houdt toezicht op jou werkzaamheden?**
   De teamleider van de afdeling P&O is degene die toezicht houdt op mijn werkzaamheden.

8. **Wat zijn de gevolgen als men verboden informatie in Compas zet?**
   Ik ben degene die het systeem beheer, maar ik zit niet in de processen van gegevensverwerking. Dus stel dat overbodige of verboden informatie in Compas wordt ingevoerd, dan moet ik samen met de teamleider van afdeling P&O bespreken wat ik daarmee kan doen.

9. **Worden de gegevens die niet meer nodig zijn verwijderd?**
   Gegevens die niet meer nodig zijn worden niet meer gebruikt of verzameld binnen Baanbrekers. De gegevens worden echter niet verwijderd. Hier is geen reden voor. Ik heb het nog nooit zien gebeuren binnen Baanbrekers.

Bijlage 9. Interview werkmakelaar in het kader van detachering
Het interview met de werkmakelaar is in deze bijlage uitgetypt. Zijn antwoorden zijn verwerkt in het onderzoeksrapport.

1. **Welke gegevens wisselen jullie uit naar de organisaties?**
   Zowel algemene persoonsgegevens zoals NAW-gegevens als bijzondere persoonsgegevens zoals gegevens omtrent de gezondheid of competenties van de sw-medewerkers worden uitgewisseld.

   Met betrekking tot de algemene persoonsgegevens, gaat het om gegevens die op de CV's van de medewerkers staan vanwege sollicitatie. Ik zorg er wel voor dat ik geen BSN stuur. Met betrekking tot de bijzondere persoonsgegevens bespreek ik en bevestig ik de competenties. Iedere werkgever vraagt wat de beperking is van een sw-medewerker. Ik geef dan aan waar men rekening mee moet houden. Ik doe dat in algemene termen van het ziektebeeld, omdat het toch van belang is voor de sw-medewerker. Ik zeg bijvoorbeeld dat bij een sw-medewerker sprake is van een lichamelijke beperkingen, maar niet dat het gaat om rugklachten.

   Uit de praktijk blijkt namelijk dat sommige sw-medewerkers geen beperkingen lijken te hebben, waardoor de externe werkgevers hen overschatten. Dit heeft een belemmerend effect of het werk van de werkgever en de werkprestatie van een sw-medewerkers.

2. **Worden deze persoonsgegevens digitaal verstuurd, per post of kunnen beide mogelijkheden?**
   - *Hoe waarborgen jullie daarbij dat persoonsgegevens niet verloren raken of door de externe organisatie onrechtmatig worden verwerkt?*
   - *Dienen zij daarvoor een geheimhoudingsverklaring te tekenen of iets dergelijks?*

   De persoonsgegevens worden zowel digitaal als per post gestuurd. Voor de waarborging wordt niets bijzonders gedaan, omdat wij ervan uitgaan dat de andere organisatie wel weet wat wij van hen verwachten. Bovendien versturen wij de gegevens altijd naar de directeur of de afdeling personeelszaken. Wij doen er geen geheimhoudingsverklaring bij. Bij psychische informatie zijn wij wel extra voorzichtig, door er bijvoorbeeld een bijsluiter bij te doen.

3. **Wordt de betrokkene geïnformeerd over:**
   - *welke gegevens er worden verstuurd;*
   - *naar welke organisatie het wordt verstuurd;*
   - *met welk doel het wordt verstuurd.*

   En zoja, gebeurd dit mondeling, is de informatie opgenomen op een brief of iets dergelijks?

   De sw-medewerkers worden door ons geïnformeerd over de gegevensuitwisseling tijdens overleg. Ook vertellen wij om welke gegevens het gaat. Bovendien dienen de sw-medewerkers bij het versturen van herindicatie te tekenen voor akkoord. Anders vervalt de indicatie.

1. **Wordt de (ondubbelzinnige) toestemming van de betrokkene gevraagd voordat de persoonsgegevens worden verstuurd?**
   - *Gebeurd dit mondeling of dient de betrokkene hiervoor iets te ondertekenen, waaruit blijkt dat akkoord is gegeven?*

   De sw-medewerkers geven toestemming wanneer zij de documenten ondertekenen. In het algemeen wordt geen toestemming gevraagd.

2. **Welke afdeling zorgt uiteindelijk voor de uitwisseling van de persoonsgegevens?**
   - *Jullie zelf, afdeling personeelsadministratie of afdeling P&O?*

   De werkmakelaars geven de documenten die bestemd zijn om te worden verstuurd aan de medewerkers van de afdeling personeelsadministratie. Deze medewerkers sturen de documenten op.

3. **Wat gebeurd er met de persoonsgegevens nadat de sw-medewerker klaar is met werken bij een externe organisatie ?**
   - *Dienen jullie nog te waarborgen dat de persoonsgegevens niet meer worden gebruikt?*
   - *Zijn jullie nog aansprakelijk in het geval de persoonsgegevens toch onrechtmatig worden verwerkt door een dergelijke organisatie?*
   - *Of vertrouwen jullie erop dat de gegevens niet meer door de organisatie verder worden verwerkt?*

   De werkmakelaars bemoeien zich niet met de administratie van de externe organisatie. Wij zijn alleen vanuit Baanbrekers voorzichtig met ziektebeelden en bevindingen van een persoon. Om die reden doen wij ook niet alles met betrekking tot de sw-medewerker in het rapport. Wanneer dergelijke documenten worden verstuurd als voortgangsrapporten of korte evaluaties met betrekking tot de sw-medewerker, dan wordt onderaan de brief standaard het volgende vermeld:

   "Cliënt heeft een kopie ontvangen
   Werkgever heeft een kopie ontvangen
   Alle informatie inzake onze deelnemers aan een re-integratietraject wordt vertrouwelijk behandeld. Iedere medewerker die vanuit zijn/haar functie met vertrouwelijke informatie in aanraking komt, heeft een geheimhoudingsplicht."

Bijlage 10. Interview juriste
Het interview met de juriste is in deze bijlage uitgetypt. Haar antwoorden zijn verwerkt in het onderzoeksrapport.

1. **Op welke manier hou jij je collega's op de hoogte van onderwerp die betrekking hebben op het privacyrecht?**
   Ik hou de medewerkers periodiek op de hoogte van veranderingen die relevant zijn voor Baanbrekers. Binnen de organisatie is een e-mailgroep. In die groep wordt gemaild over de veranderingen en wat de veranderingen gaan betekenen voor Baanbrekers. Periodiek sluit ik ook aan bij vergaderingen van de afdeling P&O.
   Tot slot kunnen de medewerkers bij mij binnenlopen om te vragen of ik documenten wil toetsen, om te kunnen beoordelen of deze conform de wet zijn.

2. **Waarom is er een aparte reglement opgemaakt en niet gewoon de Wbp genomen als geheel qua reglement?**
   Toentertijd was de Wbp niet zo uitgebreid. Het richtte zich primair alleen op de persoonsgegevens. In het algemeen waren er wel huisregels voor Baanbrekers, maar deze behandelde alleen de algemene begrippen. Het reglement is geschreven vanuit de personeelsafdeling "human reseach". Dit reglement richt zich primair ook op persoonsgegevens, maar anticipeert ook op wat er in de praktijk gebeurt. Het reglement geeft daarom ook een nadere invulling aan de Wbp.

3. **Wie is op grond van het privacyreglement personeelsadministratie de verantwoordelijke van het proces van gegevensverwerking?**
   Stel dat er op de afdeling P&O een datalek plaatsvindt, dan is de manager van Baanbrekers verantwoordelijk. Hij brengt dan verschillende afdelingen samen, waaronder de afdeling Interne Beheersing en de juriste. Samen zullen zij beoordelen of sprake is van een datalek, die zodanig groot is dat heze gemeld moet worden.

4. **Door wie en hoe wordt intern en/of extern toezicht gehouden op de naleving van het privacyreglement?**
   Vroeger werd toezicht gehouden door mij en mijn toenmalige collega. Eén of twee keer per jaar gingen wij als mystery guests rond de organisatie. Het beleid dat hiervoor gold was de "clean house policy". Wij keken waar de persoonsgegevens lagen, omdat de bureaus schoon moesten zijn. Wij hielden dus een audit. Wat wij constateerden, gaven wij door aan het managementteam. Vanuit het managementteam kwam een reminder (nu Vitamineb) naar alle medewerkers. De medewerkers bij wie het er erg aan toe was, werden ook apart bericht. De audits zijn echter gestopt toen mij collega is gestopt met werken bij Baanbrekers en ik alle juridische zaken overnam.

   Momenteel wordt geen toezicht gehouden op naleving van het privacybeleid. Ik ga ervan uit dat de leidinggevende van elke afdeling zich daarmee bezig houdt. Overigens kunnen alle medewerkers het privacybeleid ook raadplegen op het intranet, om te weten of zij eraan voldoen of niet. In de praktijk blijkt dat nauwelijks gebruik wordt gemaakt van afsluitbare kastjes. Men laat belangrijke documenten gedurende de dag en soms zelfs wanneer zij afwezig zijn, rondslingeren op kantoor. Daarnaast heeft iedereen een sleutel en dienen zij daarmee de deur op slot te doen indien zij afwezig zijn. Dit geldt dus ook voor momenten dat bijvoorbeeld pauze wordt gehouden. Ook hier wordt in veel gevallen niet aan voldaan, waardoor de ruimtes toegankelijk zijn voor iedereen. Dus ook de schoonmakers.

   Met betrekking tot de digitale dossiers geldt dat elke medewerker alleen toegang krijgt op Compas voor de dossiers die betrekking hebben op de mensen die onder haar of zijn afdeling vallen. Afdeling Interne Controle houdt toezicht in het kader van

informatieveiligheid en elk persoon die in reguliere dienst is bij Baanbrekers tekent een geheimhoudingsverklaring.

5. **Zijn er in het verleden klachten/geschillen voorgekomen omtrent de privacy?**
   Tot dusver hebben wij geen klachten gehad.

6. **Is er in het verleden sprake geweest van datalek?**
   Er is binnen Baanbrekers één keer sprake geweest van een datalek. Dit was echter niet de fout van Baanbrekers maar van de gemeente, waardoor er geen grote gevolgen zijn geweest.

7. **Nu gaat de AVG van kracht in 2018, nu hebben organisaties nog de tijd om er naartoe te werken. Hoe bereidt baanbrekers zich voor op deze richtlijn?**
   De eerste aanzetten worden ervoor gemaakt. Vroeger zou ik hiermee bezig zijn met mijn collega. Op het moment is er niemand die de tijd heeft op het privacybeleid te updaten.

Bijlage 11. Interview afdeling Interne Controle

In deze bijlage zijn twee interviews opgenomen met verschillende medewerkers van de afdeling Interne Controle. Het eerste interview (11a) heeft betrekking op de werkzaamheden van de afdeling Interne Controle. Het tweede interview (11b) heeft meer betrekking op het project informatieveiligheid.

11a.

1. **Wat de functie van een interne controle beheerder precies in?**
   Interne controle borgt dat alle bedrijfsprocessen lopen zoals deze moeten lopen. Op alle afdelingen voeren gegevensgerichte controle uit. Het gaat daarbij om alle gegevens, waaronder ook de persoonsgegevens.

2. **Welk bedrijfsproces gaat deze functie aan?**
   De afdeling Interne Controle kijkt ten eerste naar de juistheid. Daarnaast kijken wij ook naar of nieuwe wetgevingen goed worden geïmplementeerd.

3. **Gebruiken jullie voor deze functie een beleid, waarop jullie werkwijze gebaseerd is?**
   Wij werken langs het normenkader. Het normkader is afkomstig van de afdeling accountancy en onze eigen bedrijfsprocessen.

4. **Ik heb gehoord dat jullie steekproeven houden?**

- Wat is het doel daarvan
- Hoe vaak wordt het gedaan
- Op welke manier wordt het gehouden

   Steekproeven verschillen per afdeling. Momenteel worden er ongeveer 25 proeven over het hele jaar gehouden. Wij controleren de in dienst, uit dienst, verwerking van mutaties, verwerking van declaraties, salaris aanzicht, bruto (alle verschillende facetten) enzovoorts.

5. **Is het met een steekproef gelukt om informatie te ontdekken dat verboden is?**

- **En wat is het gevolg hiervan?**
  Sommige processen zijn iets dieper dan anderen. Als zoiets wordt opgemerkt, dan wordt dit in de meeste gevallen gewoon aangepast.

6. **Wordt er naast de steekproeven ook op een ander manier toezicht gehouden, zoals bijvoorbeeld doormiddel van een Mystery Guest?**

Nee, alleen onze afdeling houdt gegevensgerichte controle. Uit het jaarplan blijkt waaraan de afdeling in het komende jaar aandacht moet besteden. Daarna wordt elk kwartaal een memo voor de afdelingen gemaakt met betrekking tot de punten waar controle op is gehouden. In de memo staat wat is opgemerkt, welke wetgevingen eraan komen en in hoeverre de werkwijze van Baanbrekers voldoet aan deze wetgeving voldoet.

11 b.

Wanneer is precies met het projectgroep informatieveiligheid begonnen?
Op 13-11-2014 is de eerste kennisgeving verzonden naar het managementteam. Daarin is medegedeeld dat er het een en ander aan komt op het gebied van informatieveiligheid. Circa een half jaar later is de uitkomst van de 0-meting BIG gedeeld met het managementteam, is vervolgens het projectplan voorgelegd aan het MT (waarop in de loop der tijd nog aanvullingen plaatsvonden), is het MT geïnformeerd over de informatieveiligheid (CISO functionaris), de privacyverordening en het inzetten functionaris gegevensbescherming. In de tussentijd is informatiebeleid tot stand gekomen. Daarop zijn wij in zeer kleine kring gestart met het project. Voorafgaand hebben wij veel aan awareness gedaan om zo meer draagvlak en herkenning te creëren tijdens de start van het brede project. Rondom de zomervakantie 2016 is vervolgens met een brede projectgroep gestart. Daarin waren vertegenwoordigers betrokken van de meeste afdelingen die werken met persoonlijke informatie. Zij zijn de afgevaardigde, zij moeten communiceren met hun achterban en een en ander in werking zetten. Op basis van de vragen uit de BIG (baseline), heb ik met een collega een onderverdeling gemaakt per afdeling en die vragen uitgezet naar de afgevaardigden. Het is aan hun om de komende tijd ervoor te zorgen dat zij aan alles voldoen. Daarbij mogen zij zelf aangeven in welke volgorde en met welke prioriteit.

- **Gaat het om de informatie van Baanbrekers of van de gemeenten?**

Baanbrekers werkt op basis van een Gemeenschappelijke Regeling. Zij voert opdrachten uit voor de gemeenten. Onze klanten maken dus onderdeel uit van de gemeenten. Echter, gaat het enkel om die zaken die voortvloeien uit de GR. Dus Participatiewet (uitkeringsklanten) en medewerkers die werken bij en voor Baanbrekers.

- **De melding die gemaakt moet worden in 2017, komt dat overeen met de meldplicht datalekken?**

Wij hebben regels opgesteld omtrent de meldplicht datalekken en het feit dat we de lekken zelf registreren en waar verplicht ook melden aan de Autoriteit Persoonsgegevens.

- **De Europese richtlijnen die bij het plan wordt betrokken, is dat onder andere de Privacyrichtlijn?**

Ja. Wij proberen een aantal vliegen in één klap te vangen. Daarbij komt er straks een medewerker die uitvoerend belast is met de taken van CISO en gegevensbescherming. Daarnaast komen er op beleidsniveau 2 medewerkers die zich bezig houden met de privacyregels. Dat zijn de juriste en ik.

<u>Over het onderwerp: Algemene Verordening Gegevensbescherming</u>

- **Wat zijn tot nu toe de aanzetten tot het werken naar het voldoen aan de AVG?**

Denk hierbij aan:

- *de aanbevelingen, streefdoelen etc. die jullie al hebben of nog willen opstellen.*

Dit hebben wij nog niet zo concreet geformuleerd. Wij proberen nu vooral de basale uitgangspunten mee te nemen. Of het nu gaat om privacy of informatieveiligheid, het uitgangspunt blijft voor ons: de informatie waar wij mee werken is niet van ons maar van de persoon zelf. Dus horen wij de informatie ook als zodanig te behandelen.

- *Wie de Privacy- of securityofficer wordt en waarom is gekozen voor die persoon/afdeling?*

Zie hierboven. Bewust een onderscheid tussen privacy (beleidsmatig) en CISO/FG (operationeel). Zo geen slager die zijn eigen vlees snijdt en zo onderscheid tussen beleid en operationeel. CISO/FG komt binnen mijn afdeling: het gaat immers om interne beheersing.

Omdat privacy zeker ook een juridisch aspect heeft, gaan de juriste en ik als privacyofficers hier samen in op.

Bijlage 12 Bewerkersovereenkomst

Colofon

Naam document
Bewerkersovereenkomst

Versienummer
0.4

Versiedatum
Januari 2016

Leeswijzer

Doel
Dit document bevat een standaard bewerkersovereenkomst en een voorbeeld bijlage met maatregelen voor de bewerker die **Baanbrekers** als verantwoordelijke kan gebruiken bij het laten bewerken van persoonsgegevens.

Doelgroep
Dit document is van belang als Baanbrekers persoonsgegevens laat beheren door een derde partij, bijvoorbeeld bij een SaaS oplossing. Doelgroep is personen die te maken hebben met het uitbesteden van diensten waar persoonsgegevens worden bewerkt, bijvoorbeeld inkopers, contractbeheerders en systeemeigenaren.

Relatie met overige producten
- Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)
  - Strategische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten
  - Tactische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten
- Voorbeeld Informatiebeveiligingsbeleid van de gemeente, H2.4.1
- Beveiligingseisen in inkoopvoorwaarden
- Uitbesteding ICT-diensten
- Voorbeeld Responsible Disclosure beleid gemeenten

Maatregelen tactische variant Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)

Maatregel 6.2.1.5 Afsluiten bewerkersovereenkomst **of aan bestaande overeenkomsten een addendum in dit kader afsluiten**
Maatregel 6.2.1.6 Vastleggen beveiligingsmaatregelen in contracten
Maatregel 6.2.1.7 Rapporteren over naleving van afspraken

Inhoud

1 Inleiding

Bij het uitbesteden van de verwerking van persoonsgegevens worden door de Wet bescherming persoonsgegevens (Wbp) nadere eisen gesteld, zie Art. 14 Jo 12 en 13 Wbp. Uit deze artikelen volgt dat de verantwoordelijke[1] (in dit geval **Baanbrekers**) een schriftelijke overeenkomst dient af te sluiten met de bewerker[2] (in dit geval de derde partij), deze overeenkomst heet de bewerkersovereenkomst, **of in ieder geval een addendum c.q. bijlage moet toevoegen aan een bestaande overeenkomst met een derde partij, waarin afspraken hieromtrent worden gemaakt met de bewerker.**
De bewerker wordt door de Wbp gedefinieerd als 'degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.'

Het opstellen van een bewerkersovereenkomst dient ertoe te waarborgen dat de verplichtingen die vanuit de Wbp op de verantwoordelijke rusten, ook door de bewerker worden nageleefd. Daartoe dienen in de bewerkersovereenkomst afspraken en maatregelen te staan die de verantwoordelijke genomen wil hebben door de bewerker. Belangrijk is dat volgens de Wbp de verantwoordelijke aanspreekbaar blijft voor de gegevens die onder zijn verantwoordelijkheid door de bewerker worden verwerkt.

Voorbeelden van bewerkers zijn:
- externe leveranciers, waaronder Cloud-dienst leveranciers
- adviseurs
- accountants
- EDP-auditors
- (salaris) administrateurs.

Hoewel het lijkt dat bijvoorbeeld een SaaS[3] leverancier niet feitelijk de persoonsgegevens bewerkt, is deze toch volgens de Wbp de bewerker van persoonsgegevens als die op zijn / haar systemen staan.

Relatie met andere overeenkomsten
Het uitbesteden van werkzaamheden, de eigenlijke dienstverlening, wordt meestal in een aparte overeenkomst geregeld, hierna aangeduid met 'hoofdovereenkomst'.
De bewerkersovereenkomst regelt alleen het zorgvuldig omgaan met de persoonsgegevens die noodzakelijkerwijze bij de uitvoering van de 'hoofdovereenkomst' moeten worden verwerkt.
Dat het beschermen van persoonsgegevens in een aparte overeenkomst moet worden geregeld, volgt uit de navolgende formulering de 'Memorie van Toelichting' (Tweede Kamer, vergaderjaar 1997-1998, 25 892, nr. 3, p. 99): "De overeenkomst tussen de verantwoordelijke en de bewerker moet naar zijn aard betrekking hebben op de gegevensverwerking. Het contract mag geen betrekking hebben op een vorm van dienstverlening waar de gegevensverwerking slechts een uitvloeisel van is." Het is wel mogelijk de bewerkersovereenkomst apart op te stellen en vervolgens als bijlage op de hoofdovereenkomst op te nemen, waarbij in de hoofdovereenkomst naar deze bijlage wordt verwezen.

[1] De verantwoordelijke is volgens de Wet bescherming persoonsgegevens (Wbp) degene die het doel en de middelen voor de verwerking van persoonsgegevens bepaalt (Art. 1 sub d Wbp).
[2] De Wbp definieert de bewerker als 'degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen' (Art. 1 sub e Wbp).
[3] Zie: het document van de IBD over Cloud Computing gemeenten

Als de verantwoordelijke een bewerker inschakelt dient er op basis van de Wbp een schriftelijke overeenkomst te zijn, of dienen er vergelijkbare schriftelijke afspraken te bestaan: de zogenaamde 'bewerkersovereenkomst'. De bewerkersovereenkomst kan zelfstandig worden gebruikt maar is meestal een onderdeel van een overeenkomst met een breder bereik.[4]

De aspecten die in een (bewerkers)overeenkomst moeten worden opgenomen en duidelijk moeten zijn:

- Wie de verantwoordelijke is en wie de bewerker is.
- Welke verwerkingen de bewerker precies moet doen. Hierbij kan ook geregeld worden wat de bewerker (in ieder geval) niet mag doen.
- De bewerker mag de persoonsgegevens uitsluitend bewerken in opdracht van de verantwoordelijke. De bewerker mag dus niet zelfstandig besluiten om, in afwijking van die opdracht, de persoonsgegevens op een bepaalde manier te verwerken. Tenzij een wettelijke verplichting dat vereist.
- Dat de bewerker zelfstandig aansprakelijk is voor schade die door de bewerker is veroorzaakt en hem kan worden toegerekend. En, eventueel, dat in geval de verantwoordelijke aansprakelijk gehouden wordt voor verwerkingen van de bewerker, de verantwoordelijke een regresrecht heeft (vrijwaringsbepaling).
- Dat de bewerker voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen. De verantwoordelijke dient daartoe instructies te geven, en dient toe te zien op naleving van die maatregelen.
- Wanneer een bewerker buiten de EU gevestigd is, dient de verantwoordelijke ervoor zorg te dragen dat de bewerker het recht van het land van de verantwoordelijke nakomt (Art. 14 lid 4 Wbp).
- Dat de verantwoordelijke de mogelijkheden heeft om te controleren dat de bewerker zich (geheel) aan de overeenkomst houdt. Dit kan ook worden aangetoond met bijvoorbeeld een TPM, waarbij de verantwoordelijke de mogelijkheid van controle heeft.
- **Dat de bewerker een datalek binnen 72 uur moet melden aan de verantwoordelijke.**

De verantwoordelijke dient duidelijk aan de bewerker aan te geven welke maatregelen hij vereist voor het beschermen van de persoonsgegevens[5]. Deze maatregelen zijn voornamelijk gericht op exclusiviteit (vertrouwelijkheid) en integriteit van de gegevens van de verantwoordelijke, de beschikbaarheidseisen worden doorgaans in de SLA opgenomen.

Het College Bescherming Persoonsgegevens (CBP) biedt een aantal handreikingen ten behoeve van het opstellen van de bewerkersovereenkomst:

- Hoofdstuk 5 van de Handreiking verwerking persoonsgegevens: http://www.rijksoverheid.nl/onderwerpen/persoonsgegevens/documenten-en-publicaties/brochures/2006/07/13/handleiding-wet-bescherming-persoonsgegevens.html

[4] zie hiervoor het document Inkoop voorwaarden en beveiligingseisen van de IBD
[5] Zie bijvoorbeeld: De Richtsnoeren beveiliging van persoonsgegevens, paragraaf 4.2 en paragraaf 4.3

- De Richtsnoeren beveiliging van persoonsgegevens, paragraaf 4.2 en paragraaf 4.3: http://www.cbpweb.nl/downloads_rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf

Ook is er meer informatie te vinden over afspraken die gemaakt kunnen worden in het volgende document van Enisa, wat ook over Cloud Computing en serviceniveau's gaat. In de Annex en bijlage staan vragen die gesteld kunnen worden:
http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts

2 Bewerkersovereenkomst Baanbrekers

2.1 Algemeen

Deze bewerkersovereenkomst bevat generieke bepalingen die betrekking hebben op het naleven van de Wbp door de bewerker en niet op het naleven van andere wet- en regelgeving met betrekking tot persoonsgegevens, zoals de BRP- en SUWI-wetgeving. Uit deze wetgeving kunnen specifieke eisen voortvloeien, die in dit model niet zijn meegenomen.

Houd in gedachten dat verwerkingen die bijvoorbeeld vanwege de aard van de persoonsgegevens of de verwerkingen zelf met hogere waarborgen omkleed dienen te worden, niet in deze bewerkersovereenkomst vervat zijn.

Deze bewerkersovereenkomst is gebaseerd op de BIG.

De bewerkersovereenkomst is nu generiek opgezet, echter er kunnen verschillende persoonsgegevens in verschillende systemen staan, waarmee de generiek**e** eisen dus ook niet overal van toepassing hoeven te zijn. Bedenk wel dat de gemeenten en hun uitvoeringsorganisaties, **zoals Baanbrekers**, uiteindelijk allemaal ergens aan elkaar hangen en dat sommige gegevens die uit ketens afkomstig zijn, minimaal beveiligd moeten worden met eenzelfde niveau aan maatregelen tegen de risico's die er zijn.

Deze bewerkersovereenkomst is ook te gebruiken als algemeen model met afspraken tussen Baanbrekers en een leverancier.

Wet bescherming persoonsgegevens (Wbp) bewerkersovereenkomst

Deze bewerkersovereenkomst vormt een onlosmakelijk onderdeel van de overeengekomen overeenkomst tussen Baanbrekers en (NAAM BEWERKER) inzake (NOEMEN DE DIENSTVERLENING DIE BEWERKER VOOR BAANBREKERS VERRICHT), DATUM (VERMELDEN DE DATUM VAN HET GESLOTEN CONTRACT).

Het Dagelijks Bestuur van Baanbrekers, rechtsgeldig vertegenwoordigd door NAAM (Evt. Functie/manager of directeur), gevestigd aan de Zanddonkweg 14, 5144 NX te Waalwijk, verder te noemen de verantwoordelijke,

en

NAAM organisatie bewerker, rechtsgeldig vertegenwoordigd door NAAM (evt. functie), gevestigd aan de ADRES, PC en PLAATS, verder te noemen de bewerker,

verklaren te zijn overeengekomen een bewerkersovereenkomst als bedoeld in artikel 14, tweede lid, van de Wbp**, tussen Baanbrekers**, nader te noemen de verantwoordelijke en <nader in te vullen naam van de bewerker>, nader te benoemen de bewerker.

Definities

Artikel 1.

1.1 Bijlagen: aanhangsels bij deze overeenkomst, die na door beide partijen te zijn geparafeerd, deel uitmaken van deze overeenkomst.

1.2 Normen en standaarden: de door de verantwoordelijke vastgestelde normen en standaards ter zake van methoden, technieken, procedures, projecten, productiekenmerken en documentatievoorschriften welke bij de uitvoering van de werkzaamheden door de bewerker zullen worden **gevolgd als vastgelegd in bijlage 2**. Ik zie geen bijlage 2 bij deze overeenkomst. Wat is dit? Bovendien wordt in punt 6.1. van deze overeenkomst i n dit kader gesproken over bijlage 1??????????????????

1.3 Verwerking van persoonsgegevens of het verwerken van persoonsgegevens: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bewerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, evenals het afschermen, uitwissen of vernietigen van gegevens.

1.4 Bestand: elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen.

1.5 Verantwoordelijke: de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

1.6 Bewerker: degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.

1.7 Betrokkene: degene op wie een persoonsgegeven betrekking heeft.

1.8 Derde: ieder, niet zijnde de betrokkene, de verantwoordelijke, de bewerker, of enig persoon die onder rechtstreeks gezag van de verantwoordelijke of de bewerker gemachtigd is om persoonsgegevens te verwerken.

1.9 Ontvanger: degene aan wie de persoonsgegevens worden verstrekt.

1.10 Toestemming van de betrokkene: elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt.

1.11 Het College bescherming persoonsgegevens of het College: het College als bedoeld in artikel 51 van de Wbp.

1.12 Functionaris: de functionaris voor de gegevensbescherming als bedoeld in artikel 62 van de Wbp.

1.13 Voorafgaand onderzoek: een onderzoek als bedoeld in artikel 31 van de Wbp.

1.14 Verstrekken van persoonsgegevens:- het bekend maken of ter beschikking stellen van persoonsgegevens.

Ingangsdatum en duur

Artikel 2.

2.1 Deze overeenkomst gaat in op het moment van ondertekening **en duurt voort zolang de overeenkomst datum XXXX zoals overeengekomen tussen verantwoordelijke en bewerker voortduurt, en zo lang bewerker als bewerker van ter beschikking gestelde persoonsgegevens door verantwoordelijke optreedt**.

Onderwerp van deze overeenkomst

Artikel 3.

3.1 De bewerker verwerkt persoonsgegevens in opdracht van de verantwoordelijke in het kader van de uitvoering van <**Overeenkomst datum XXXX, inzake WELKE DIENSTVERLENING/activiteiten >.**

3.2 De bewerker verbindt zich om in het kader van die werkzaamheden de door de verantwoordelijke ter beschikking gestelde persoonsgegevens zorgvuldig te verwerken.

3.3 Dat de Wbp aan de verantwoordelijke de plicht oplegt om ervoor zorg te dragen dat de bewerker voldoende waarborgen biedt ten aanzien van de technische- en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen.

Naleving wet- en regelgeving

Artikel 4.

4.1 Het **Dagelijks Bestuur** van Baanbrekers is verantwoordelijke in de zin van de Wbp.

4.2 **De directeur en managers** van Baanbrekers zijn namens de verantwoordelijke belast met het beheer van de binnen Baanbrekers in beheer zijnde gegevensverwerkingen.

4.3 De bewerker verwerkt gegevens ten behoeve van de verantwoordelijke, in overeenstemming met diens instructies.

4.4 De bewerker heeft geen zeggenschap over de ter beschikking gestelde persoonsgegevens. Zo neemt hij geen beslissingen over ontvangst en gebruik van de gegevens, de verstrekking aan derden en de duur van de opslag van gegevens. De zeggenschap over de persoonsgegevens verstrekt onder deze overeenkomst komt nimmer bij de bewerker te berusten.

4.5 De bewerker zal bij de verwerking van persoonsgegevens in het kader van de in artikel **3.1** genoemde **werkzaamheden/dienstverlening of activiteiten,** handelen in overeenstemming met de toepasselijke wet- en regelgeving betreffende de bescherming van persoonsgegevens. De bewerker verwerkt persoonsgegevens slechts in opdracht van **NAAM CONTACTPERSOON BAANBREKERS (Naam MANAGER OF DIRECTEUR van BB)** en zal alle redelijke instructies dienaangaande opvolgen, behoudens afwijkende wettelijke verplichtingen.

4.6 De bewerker zal onmiddellijk bij het ontdekken van beveiligingsinbreuken of datalekken deze melden aan de **in 4.5. genoemde contactpersoon van** verantwoordelijke, al dan niet onder verbeurte van een boete in geval van niet-nakoming, conform artikel 9.3 van deze overeenkomst.

4.7 De bewerker zal te allen tijde op eerste verzoek van **Baanbrekers** onmiddellijk alle van **Baanbrekers** afkomstige persoonsgegevens met betrekking tot deze bewerkersovereenkomst ter hand stellen.

4.8 De bewerker zal alle van de verantwoordelijke afkomstige persoonsgegevens met betrekking tot deze bewerkersovereenkomst op een nader te bepalen wijze vernietigen op het moment van beëindigen van deze overeenkomst, dan wel op uitdrukkelijk verzoek van de verantwoordelijke de gegevens te vernietigen op een nader te bepalen wijze.

4.9 De bewerker stelt de verantwoordelijke te allen tijde in staat om binnen de wettelijke termijnen te voldoen aan de verplichtingen op grond van de Wbp, meer in het bijzonder de rechten van betrokkenen, zoals, maar niet beperkt tot een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens en het uitvoeren van een gehonoreerd aangetekend verzet.

Geheimhoudingsplicht

Artikel 5.

5.1 Personen in dienst van, dan wel werkzaam ten behoeve van de bewerker, evenals de bewerker zelf, zijn verplicht tot geheimhouding met betrekking tot de persoonsgegevens waarvan zij kennis kunnen nemen, behoudens voor zover een bij, of krachtens de wet gegeven voorschrift tot verstrekking verplicht of zijn taak daartoe noodzaakt. De medewerkers van de bewerker tekenen hiertoe een geheimhoudingsverklaring **of hebben hiertoe schriftelijk een geheimhoudingsverplichting opgelegd gekregen.**

5.2 Indien de bewerker op grond van een wettelijke verplichting gegevens dient te verstrekken, zal de bewerker de grondslag van het verzoek en de identiteit van de verzoeker verifiëren en zal de bewerker **de genoemde contactpersoon van Baanbrekers** onmiddellijk, voorafgaand aan de verstrekking, ter zake informeren. Tenzij wettelijke bepalingen dit verbieden.

Beveiligingsmaatregelen

Artikel 6.

6.1 De bewerker neemt alle passende technische en organisatorische maatregelen om de persoonsgegevens welke worden verwerkt ten dienste van de verantwoordelijke te beveiligen en beveiligd te houden tegen verlies of tegen enige vorm van onzorgvuldig, ondeskundig of ongeoorloofd gebruik. **Tevens verklaart de bewerker zich te houden aan de normen en standaards van de verantwoordelijke, zoals beschreven in bijlage 1**. Ik zie geen bijlage 1 bij deze overeenkomst?????????????????????????? In 1.2. ook naar zoiets verwezen?

6.2 De verantwoordelijke is te allen tijde gerechtigd om de verwerking van persoonsgegevens te controleren. De bewerker is verplicht de verantwoordelijke of controlerende instantie in opdracht van verantwoordelijke toe te laten en verplicht medewerking te verlenen zodat de controle daadwerkelijk uitgevoerd kan worden.

6.3 De verantwoordelijke zal de audit slechts (laten) uitvoeren na een voorafgaande schriftelijke melding aan de bewerker.

6.4 De bewerker verbindt zich om binnen een door de verantwoordelijke te bepalen termijn de verantwoordelijke, of de door de verantwoordelijke ingeschakelde derde, te voorzien van de verlangde informatie. Hierdoor kan de verantwoordelijke, of de door de verantwoordelijke ingeschakelde derde, zich een oordeel vormen over de naleving door de bewerker van deze overeenkomst. De verantwoordelijke, of de door de verantwoordelijke ingeschakelde derde, is gehouden alle informatie betreffende deze controles vertrouwelijk te behandelen.

6.5 Bewerker staat er voor in, de door de verantwoordelijke of ingeschakelde derde, aangegeven aanbevelingen ter verbetering binnen de daartoe door de verantwoordelijke te bepalen termijn uit te voeren.

6.6 De bewerker rapporteert jaarlijks over de opzet en werking van het stelsel van maatregelen en procedures, gericht op naleving van deze overeenkomst.

Inschakeling derden

Artikel 7.

7.1 De bewerker is slechts gerechtigd de uitvoering van de werkzaamheden geheel of ten dele uit te besteden aan derden na voorafgaande schriftelijke toestemming van de verantwoordelijke.

7.2 De verantwoordelijke kan aan de schriftelijke toestemming voorwaarden verbinden, op het gebied van geheimhouding en ter naleving van de verplichtingen uit deze bewerkersovereenkomst.

7.3 De bewerker blijft in deze gevallen te allen tijde aanspreekpunt en verantwoordelijk voor de naleving van de bepalingen uit deze bewerkersovereenkomst.

Wijziging overeenkomst

Artikel 8.

8.1 Wijziging van deze overeenkomst kan slechts schriftelijk plaatsvinden middels een door beide partijen geaccordeerd voorstel.

8.2 Zodra de samenwerking is beëindigd, vernietigt bewerker de persoonsgegevens die hij van de verantwoordelijke heeft ontvangen, in welke vorm dan ook en toont dit aan, tenzij partijen iets anders overeenkomen. Deze vernietiging moet, binnen nader overeen te komen termijn, uitgevoerd worden en hiervan wordt een verslag gemaakt.

8.3 Elk van de partijen is gerechtigd de overeenkomst met onmiddellijke ingang te beëindigen in geval van overmacht, waaronder mede begrepen een zodanige wijziging van wettelijke regels dat een verdere voortzetting van de overeenkomst niet kan worden verlangd.

8.4 Bij het beëindigen van de overeenkomst met onmiddellijke ingang, wordt in de brief aan de bewerker de reden van beëindiging vermeld.

Aansprakelijkheid

Artikel 9.

9.1 Indien de bewerker tekortschiet in de nakoming van de verplichting uit deze overeenkomst kan verantwoordelijke hem in gebreke stellen. Bewerker is echter onmiddellijk in gebreke als de nakoming van desbetreffende verplichting anders dan door overmacht binnen de overeengekomen termijn, reeds blijvend onmogelijk is. Ingebrekestelling geschiedt schriftelijk, waarbij aan de bewerker een redelijke termijn wordt gegund om alsnog haar verplichtingen na te komen. Deze termijn is een fatale termijn. Indien nakoming binnen deze termijn uitblijft, is bewerker in verzuim.

9.2 Bewerker is aansprakelijk voor alle schade of nadeel voortvloeiende uit het niet-nakomen van, of in strijd handelen met de bij of krachtens de Wbp gegeven voorschriften en/of het niet-nakomen van, of in strijd handelen met het in deze overeenkomst bepaalde. Onverminderd de aanspraken op grond van wettelijke regels. Bewerker is aansprakelijk voor schade of nadeel voor zover ontstaan door zijn werkzaamheid. Bewerker is tevens aansprakelijk voor alle schade of nadeel voortvloeiende uit de door zijn werkzaamheid ontstane inbreuken op de persoonlijke levenssfeer van betrokkenen.

9.3. OPTIONEEL: Indien bewerker **de genoemde verplichting(en) in de artikelen 4, 5, 6, en 7 van deze overeenkomst** niet tijdig nakomt, is bewerker een boete verschuldigd**, groot € 5.000,-per dag** zonder dat hiervoor een aanmaning of een voorafgaande verklaring nodig is. Deze boete is niet vatbaar voor verrekening en opschorting en laat het recht van verantwoordelijke op nakoming en schadevergoeding onverlet.
P.s. ik kan me voorstellen dat als ons risico groter is dit bedrag ook wordt verhoogd!

Toepasselijk recht

Artikel 10.

10.1 Op deze overeenkomst en op alle geschillen die daaruit mogen voortvloeien of daarmee mogen samenhangen, is het Nederlands recht van toepassing.

Citeertitel

Artikel 11.

11.1 Deze overeenkomst kan worden aangehaald als **“Wet bescherming persoonsgegevens Bewerkersovereenkomst”.**

Aldus in tweevoud opgesteld en getekend DATUM

Namens het dagelijks bestuur
Baanbrekers,

Naam DIRECTEUR/MANAGER

Naam BEWERKER

Naam ondertekeningsbevoegde.

> Informatiesysteem-autorisatieaanvraagformulier

(formulier s.v.p. invullen met de PC i.v.m. duidelijkheid)

Bij een onduidelijke ingevuld aanvraag formulier of niet ondertekend door de Manager, wordt deze niet in behandeling genomen en terug gestuurd

Team: ____ Functie: ____ Ingangsdatum account: ____

Personeels Nr. : ____ Afd. Nr. : ____ Aanstelling: ____

Roepnaam ____ Voorletters: ____ Achternaam: ____

Werkplek
- ☐ Nieuwe Gebruiker
- ☐ Wijziging
- ☐ Thuiswerken - eToken

- ☐ Nieuwe Werkplek
- ☐ Bestaande Werkplek

Locatie : ____

Telefonie
- ☐ Vaste telefonie
- ☐ Dect telefoon
- ☐ Extern bereikbaar
- ☐ Standaard GSM
- ☐ Smartphone
  - ☐ + Internet

Bel buget : € ____

- ☐ Identiteitsbewijs
- ☐ Locker

- ☐ Sleutel Sleutel nr.: ____
- ☐ Toegangs druppel
  - ☐ Gebouw 1
  - ☐ Gebouw 2
  - ☐ Gebouw 3
  - ☐ Pakeren

E-mail ◯ Ja ◯ Nee E-mail extensie ____

Naam aanvrager: ____

Akkoord Manager: ____

Paraaf: ____ Datum: ____

Standaard wordt geïnstalleerd:

Home Directory, Netwerkschijven, Internet, Calculator, Notepad, Adobe reader, Intranet, Handboek
Office: Word, Excel, Outlook en Power Point.
alle gebruikers krijgen standaard de zwart/wit printer.

Applicaties	Akkoord:
☐ Compas	*
☐ Navision	*
Profiel:	
☐ Adobe Photoshop	
☐ Adobe Acrobat	
☐ WSP	*
☐ Bartender	
☐ DocZend	

Applicaties	Akkoord:
☐ Liaan Frauderegistratie	*
☐ Liaan Inlichtingenbureau	*
☐ Postregistratie	*
☐ Xential	*
☐ Centric Portal	
☐ Cognos	*
☐ Suite4Wiz (Productie)	*
Profiel:	
☐ Key2BM GWS	*
☐ Key2Datadistributie	*
☐ Key2GBA-V	*
☐ Key2VOA	*
☐ SQLTools	*
☐ GWS4ALL	*
☐ Suwinet-Inkijk	*
Profiel:	
☐ Suwinet-Ib-groep	*
☐ Suwinet-WIS	*
☐ Handboek Schulinck	*

Applicaties	Akkoord:
☐ Groenvision	*
☐ Infogroen	
☐ Kalkulatie	
☐ Relatie	
☐ Kenmerk	
☐ Repond	
☐ Helix CAD	
☐ iReport	*

* **LETOP!!!**

Geheimhoudingsverklaring is noodzakelijk

- ☐ aanwezig in het personeels dossier

Printer
- ☐ Kleuren printer
- ☐ HP printer

☐ Testomgeving Beschrijf hieronder welke pakket :

Opmerking :

Datum in: ____

Verwerkt door: ____

Formulier Opslaan

Formulier afdrukken

Versie 14

P.S. Graag 5 werkdagen voor ingangsdatum account aanleveren
Niet of gedeeltelijke ingevulde opties worden niet geconfigureerd

Bijlage 14. Geheimhoudingsverklaring

Naam en voorletters : _____

Geboortedatum : _____-_____-_____

Adres : _____

Postcode en woonplaats : _____

Hierbij verklaart ondergetekende:

1. Dat hij zich bewust is van zijn verplichtingen tegenover onbevoegden strikte geheimhouding te betrachten ten aanzien van alles wat hem ten gevolge van zijn dienstbetrekking of detachering of inlening bekend wordt, zowel voor wat betreft informatie, (persoons-)gegevens, afbeeldingen en/of overige documenten van Baanbrekers, en waarvan hij weet of kan vermoeden dat een en ander van vertrouwelijk aard is. Deze verplichtingen bestaat niet tegenover hem aan wie hij onmiddellijk of middellijk ondergeschikt is, noch in zover hij van de verplichting tot geheimhouding door het hiertoe bevoegde orgaan van Baanbrekers is ontheven.

2. Dat hij zich beperkt tot enkel het eigen gebruik van het computersysteem van Baanbrekers uit hoofde van zijn functie c.q. werkzaamheden onder gezag en toezicht van Baanbrekers, en dit systeem volgens de geldende voorschriften en instructies gebruikt, waarbij hij bekend is met het gegeven dat alle bevragingen in het computersysteem worden gelogd en gecontroleerd.

3. Dat hij, voor zover nodig, hierbij nadrukkelijk op zijn verplichtingen en verantwoordelijkheden tot het gebruik van het computersysteem, de beveiliging en geheimhouding van deze informatie, (persoons-)gegevens, afbeeldingen, en/of overige documenten is gewezen.

4. Dat hij zich bewust is dat bij overplaatsing in, of detachering naar een andere interne functie, dan wel bij beëindiging van zijn dienstverband, detachering of inlening de door hem hierbij aanvaarde verplichtingen van kracht blijven, en hij onderworpen blijft aan sancties, zowel voortvloeiend uit de rechtspositieregeling en/of bij de wet gesteld. Dit voor het geval hij deze informatie, (persoons-)gegevens, afbeeldingen, en/of overige documenten opzettelijk of uit onachtzaamheid niet beveiligd of ter kennis van onbevoegden doet toekomen.

5. Dat hij bekend is met de mogelijkheid tot het opleggen van disciplinaire maatregelen, waaronder ontslag om dringende reden, of vervolging op basis van schending van de artikelen bij wet gesteld bij niet naleving van de beveiligingsbepalingen en/of de schending van de geheimhoudingsplicht.

6. Dat hij erkent een exemplaar van deze verklaring te hebben ontvangen en dat met deze ondertekende verklaring betreffende genoemde onderwerpen alle eerdere verklaringen aangaande dezelfde onderwerpen komen te vervallen.

> Geheimhoudings-gebruikersverklaring

Waalwijk, datum ___-____-_____ Handtekening:_____

Bijlage 15. Principes PIA

Voor de uitvoering van de PIA is in deze bijlage uitgebreid behandeld wat de PIA inhoudt en wat voor functie dit instrument heeft. De beschrijving van de PIA is overgenomen van het 'Toetsmodel Privacy Impact Assessment (PIA)' van de Rijksdienst. Uit dit toetsmodel zijn onderdelen overgenomen die relevant zijn voor Baanbrekers. Daarnaast zijn in deze bijlage principes uitgewerkt, die Baanbrekers bij het uitvoeren van de PIA in acht dient te nemen. Deze bijlage is uitsluitend bedoeld om nadere toelichting te geven aan de PIA en de uitvoering van dit instrument.

Wat is een PIA?

1. Een Privacy Impact Assessment (PIA) is een hulpmiddel om bij ontwikkeling van beleid, en de daarmee gepaard gaande wetgeving of bouw van ICT-systemen en aanleg van databestanden, privacyrisico's op gestructureerde en heldere wijze in kaart te brengen.
2. Een PIA is geen vrijblijvende enquête. In het bijzonder is de vragenlijst inhoudelijk gezien zowel richtinggevend als corrigerend bedoeld. Daarnaast moet het beantwoordingsproces als zodanig ook bewustwording stimuleren van de uiteenlopende privacy-aspecten waarmee rekening moet worden gehouden bij ontwikkeling van een wetgeving en beleid en in dat kader te ontwikkelen ICT- systemen en databestanden.
3. Een PIA is richtinggevend in de zin dat de (uitputtende) vragenreeks kan wijzen op relevante privacy-risico's die in de vroege fase van beleids- of systeemontwikkeling (wellicht nog) niet zijn onderkend. Als dat het geval is, moet de betreffende vraag zo worden opgevat dat het noodzakelijk is om deze aspecten alsnog in de uitwerking mee te nemen.
4. Een PIA is ook corrigerend. Door de vragenvolgorde zal het vaak nodig zijn voorlopige antwoorden op eerdere vragen te heroverwegen, en vervolgens voor een andere (minder privacy-inperkende) oplossing te kiezen. Het zal dan ook geregeld voorkomen dat in een eerder stadium van beleids- of systeemontwikkeling overwogen opties en oplossingen bij nadere beschouwing niet goed genoeg kunnen worden onderbouwd vanwege de hiermee gepaard gaande privacy-risico's.
5. Vanwege het richtinggevende en corrigerende karakter van een PIA zal het invullen van de vragenlijst vaak een dynamisch proces zijn, waarbij concept-(beleids)oplossingen of het concept-functionele systeemontwerp geleidelijk worden aangescherpt.

Principes die in acht moeten worden genomen bij de uitvoering:

- Bepaal wie de betrokkene partijen zijn bij de uitvoering van de PIA en hoe de uitvoering moet gebeuren;
- Verzamel en bestudeer relevante informatie;
- Vul de PIA vragenlijst in;[1]
- Beoordeel de impact en bedenk waar nodig (aanvullende) maatregelen;
- Stel de resultaten van de PIA vast in een PIA-rapport.

[1] drs. E. König & W. Karssenberg, 'Privacy Impact Assessment (PIA)', Amsterdam: NOREA Kennisgroep Privacy 2015, pagina 22 tot en met 45.