INFORMATIE
BEVEILIGINGS
DIENST

MODEL VOOR EEN BEWERKERSOVEREENKOMST

Een van de producten van de operationele variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN **IN OPDRACHT VAN**
VERENIGING VAN NEDERLANDSE GEMEENTEN

INFORMATIE
BEVEILIGINGS
DIENST

Colofon

Naam document
Bewerkersovereenkomst.

Versienummer
2.2.1

Versiedatum
augustus 2016

Versiebeheer
Het beheer van dit document berust bij de Informatiebeveiligingsdienst voor gemeenten (IBD).

Met dank aan
De expertgroep en de reviewgemeenten die hebben bijgedragen aan het vervaardigen van dit product.

Wijzigingshistorie:

Versie	Datum	Opmerkingen
1	18-02-2014	Eerste versie van de BIG
1.2	11-04-2016	Aanpassingen, lijst met met voorbeeld maatregelen aangepast
2.0	03-05-2016	Inleiding, Meldplicht Datalekken toegevoegd en tekstuele aanpassingen
2.1	17-06-2016	artikel 10 aangescherpt op WBP
2.2	29-07-2016	Toevoeging model (titel) en aanpassing voor de BRP en een eerste stap richting AVG en nu meer modulair van opzet.
2.2.1	19-08-2016	Tekstuele aanpassingen

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

INFORMATIE
BEVEILIGINGS
DIENST

Voorwoord

De IBD is een gezamenlijk initiatief van de Vereniging van Nederlandse Gemeenten (VNG) en het Kwaliteitsinstituut Nederlandse Gemeenten (KING). De IBD is de sectorale CERT / CSIRT voor alle Nederlandse gemeenten en richt zich op (incident)ondersteuning op het gebied van informatiebeveiliging. De IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum (NCSC). De IBD beheert de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en geeft regelmatig kennisproducten uit. Daarnaast faciliteert de IBD kennisdeling tussen gemeenten onderling, met andere overheidslagen, met vitale sectoren en met leveranciers.

De IBD heeft de volgende doelen:

1. het preventief en structureel ondersteunen van gemeenten bij het opbouwen en onderhouden van bewustzijn als het gaat om informatiebeveiliging.
2. het leveren van integrale coördinatie en concrete ondersteuning op gemeente specifieke aspecten in geval van incidenten en crisissituaties op het vlak van informatiebeveiliging.
3. het bieden van gerichte projectmatige ondersteuning op deelgebieden om informatiebeveiliging in de praktijk van alle dag naar een hoger plan te tillen. De ondersteuning die de IBD biedt bij het ICT-Beveiligingsassessment DigiD is een voorbeeld van een dergelijk project.
4. het faciliteren van kennisdeling tussen gemeenten op het vlak van informatiebeveiliging.

Hoe realiseert de IBD haar doelen?
Om invulling te kunnen geven aan haar doelen is door de IBD op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR) een vertaalslag gemaakt naar een baseline voor de gemeentelijke markt. Deze Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) betreft twee varianten, een Strategische- én een Tactische Baseline. Beide varianten van de BIG zijn beschikbaar voor alle gemeenten op de community van de IBD, zodat door iedere gemeente tot implementatie van de BIG kan worden overgegaan. Bestuur en management hebben met deze baseline een instrument in handen waarmee zij in staat zijn om te meten of de organisatie 'in control' is op het gebied van informatiebeveiliging. Om de implementatie van de Strategische en Tactische Baseline te ondersteunen, zijn door de IBD in samenwerking met de Taskforce Bestuur en Informatieveiligheid Dienstverlening producten ontwikkeld op operationeel niveau. Dit heeft een productenportfolio opgeleverd, genaamd de Operationele Baseline Nederlandse Gemeenten. Onderhavig product is er één van.

Naast een productenportfolio, heeft de IBD voor gemeenten ook een dienstenportfolio ontwikkeld. Voor een volledig overzicht van het producten- en dienstenportfolio, kunt u terecht op de website van de IBD.

De gemeente is zelf verantwoordelijk voor het opstellen en/of uitvoeren en/of handhaven van de regels. Hierbij gelden de volgende uitgangspunten:

- Er is wetgeving waar altijd aan voldaan moet worden, zoals niet uitputtend: BRP, Wbp, SUWI, BAG en PUN, maar ook de archiefwet.
- Er is een gemeenschappelijk normenkader als basis: de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).
- De gemeente stelt dit normenkader vast, waarbij er ruimte is in de naleving van dat kader voor afweging en prioritering op basis van het 'pas toe of leg uit' principe.

Leeswijzer

Dit product maakt onderdeel uit van de operationele variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

Doel
Dit product bevat een model voor een bewerkersovereenkomst, het model kan gebruikt worden voor de Wbp (art. 14) en/of voor de BRP (art. 7 Besluit basisregistratie personen).
LET OP: bij de toelichting en de overeenkomst zelf staat de Wbp op de voorgrond! Als u het model voor de BRP gebruikt moet u bedacht zijn op de juiste verwijzigingen naar de BRP en moet u duidelijk maken dat het Besluit en de Regeling BRP altijd geldt.

Doelgroep
Dit document is van belang als de gemeente persoonsgegevens laat beheren door een derde partij, bijvoorbeeld bij een SaaS oplossing. De doelgroep bestaat uit 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
- Inkoopvoorwaarden en informatiebeveiligingseisen
- Toegang van externe partijen en inhuur
- Handreiking Service Level Agreements
- Geheimhoudingsverklaringen
- Handleiding screening personeel
- Contractmanagement
- Responsible Disclosure

Maatregelen tactische variant Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)

Maatregel 6.2.1.5 Afsluiten bewerkersovereenkomst
Maatregel 6.2.1.6 Vastleggen beveiligingsmaatregelen in contracten
Maatregel 6.2.1.7 Rapporteren over naleving van afspraken

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

Inhoud

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN
VERENIGING VAN NEDERLANDSE GEMEENTEN

1 Aanleiding

Bij de dienstverlening en bedrijfsvoering van gemeenten worden persoonsgegevens verwerkt. De gemeentelijke dienstverlening is een integraal onderdeel van procesketens, zoals bijvoorbeeld op het gebied van de jeugdzorg, maatschappelijke ondersteuning, werk en inkomen, de registratie van personen, gebouwen en adressen en de uitgifte van persoonsdocumenten. Gemeenten werken als meest nabije overheidslaag bij de uitvoering van hun taken ook veelvuldig samen met andere overheidsorganisaties, semioverheidsorganisaties en bedrijven. Bij de verwerking van persoonsgegevens is het van belang en zelfs wettelijk verplicht de afspraken en verantwoordelijkheden hieromtrent vast te leggen. Deze afspraken worden vastgelegd in een zogenaamde bewerkersovereenkomst.

Bij het opstellen van een bewerkersovereenkomst zijn verschillende belangen gemoeid waarbij risico's en aansprakelijkheid op een redelijke wijze moeten worden toegewezen aan de verschillende partijen.

De voorliggende voorbeeldovereenkomst biedt gemeenten een handvat en een uitgangspunt om de eigen specifieke bewerkersovereenkomst vorm te geven.

Deze bewerkersovereenkomst is gebaseerd op het gemeenschappelijke normenkader voor informatiebeveiliging, de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG), en is tot stand gekomen op basis van voorbeelden van onder meer de gemeente Amsterdam en een aantal leveranciers.

1.1 Wettelijk kader

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 de gemeente) een schriftelijke overeenkomst dient af te sluiten met de bewerker[2] (in dit geval de derde partij), deze overeenkomst heet de bewerkersovereenkomst. 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.'
Hetzelfde geldt bij het uitbesteden van de verwerking van persoonsgegevens die onder de BRP vallen, zie de artikelen 6 t/m 9 van het Besluit BRP en de artikelen 5 en 6 van de Regeling BRP.

1.2 Doelstelling

Het opstellen van een bewerkersovereenkomst dient ertoe te waarborgen dat de verplichtingen die vanuit de Wbp/BRP op de verantwoordelijke rusten, ook door de bewerker worden nageleefd. Daartoe dienen in de bewerkersovereenkomst afspraken en maatregelen te staan die de verantwoordelijke (bij de BRP het College) genomen wil hebben door de bewerker. Belangrijk is dat

[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).

volgens de Wbp de verantwoordelijke aanspreekbaar blijft voor de gegevens die onder zijn verantwoordelijkheid door de bewerker worden verwerkt.

Voorbeelden van bewerkers zijn:
- externe ICT-leveranciers, waaronder Cloud-dienst leveranciers
- externe (salaris) administrateurs
- externe partijen waaraan gemeentelijke werkzaamheden zijn uitbesteed en waarbij persoonsgegevens verwerkt worden.

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

Accountants, auditors en adviseurs worden verantwoordelijke, ze bewerken en verwerken geen gegevens, ze krijgen die alleen tijdelijk voor controle doeleinden. Geheimhouding en vernietiging naar twee jaar volstaat voor deze doelgroepen. In bijzondere gevallen mogen ze gegevens op locatie inzien (medisch/strafrecht e.d.).

1.3 Verantwoording afleggen

De verantwoordelijke dient passende en aantoonbare technische en organisatorische maatregelen uit te voeren met als doel ervoor te zorgen dat de verwerking van persoonsgegevens in overeenstemming is met geldende wet- en regelgeving en daarover transparant te zijn. De verantwoordelijke dient hierover verantwoording af te kunnen leggen (accountable), maar ook gecontroleerd kunnen worden (auditable). Het is hierbij van belang om hierover met de bewerker goede afspraken te maken, zodat de verantwoordelijke aan zijn wettelijke verplichtingen kan voldoen. Dit betekent dat men documentatie dient te hebben waarin uitgebreid alle aspecten van de verwerking van persoonsgegevens door de verantwoordelijke worden beschreven. Om hieraan te kunnen voldoen dient de verantwoordelijke hierover goede afspraken te maken met de bewerker.

Eén van de beveiligingsmaatregelen die de activiteiten met betrekking tot de verwerking van persoonsgegevens kunnen onderbouwen is logging en de daaraan gerelateerde controle. Denk hierbij aan het vastleggen in logbestanden van alle activiteiten die gebruikers en beheerders uitvoeren, informatiebeveiligings- en andere relevante gebeurtenissen, zoals pogingen van ongeautoriseerde toegang. Deze logbestanden dienen gedurende een overeengekomen periode te worden bewaard, ten behoeve van toekomstig onderzoek, en dienen periodiek te worden gecontroleerd op indicaties van onrechtmatige toegang of onrechtmatig gebruik. Waar nodig dienen noodzakelijke acties te worden ondernomen.

Verantwoordelijke hebben logging nodig om zich te kunnen verantwoorden tegenover de betrokkene, toezichthouders en anderen, over de zorgvuldigheid waarmee zij met de persoonsgegevens omgaan (transparantie). Bij de beheersing van toegang tot persoonsgegevens vormt de logging, als vastlegging van feitelijke gebeurtenissen, een belangrijke schakel. Het loggen maakt verantwoording en controle achteraf mogelijk. De controle van deze logging kan op verschillende plekken plaatsvinden afhankelijk van de mate van uitbesteding. In ieder geval moet

[3] Zie: het document van de IBD over Cloud Computing gemeenten

de verantwoordelijke voldoen aan de plicht om te controleren wie welke gegevens ingezien dan wel bewerkt heeft, maar als de bewerker ook handelingen verricht, naast beheer (bijvoorbeeld bij een proces uitbesteding) dan dient de bewerker diezelfde controle voor wat betreft zijn eigen personeel uit te voeren en daarover actief te rapporteren aan de verantwoordelijke. Het gaat erom dat, ongeacht waar welke werkzaamheden uitgevoerd worden, altijd te controleren is of er persoonsgegevens rechtmatig en proportioneel verwerkt zijn. De verantwoordelijke kan niet voldoen aan zijn verantwoordelijkheid als er geen sluitende controle plaatsgevonden heeft.

1.4 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 slechts de zorgvuldige omgang met de persoonsgegevens die noodzakelijkerwijs bij de uitvoering van de 'hoofdovereenkomst' moeten worden verwerkt.

Voor de te maken afspraken met de bewerker, wordt meestal een bewerkersovereenkomst afgesloten waarbij deze de (hoofd)overeenkomst aanvult.
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 (soort) persoonsgegevens worden verwerkt en eventueel de wettelijke basis.
- 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.
- Het model is bedoeld voor bewerkers die in Nederland gevestigd zijn, als de bewerker niet in Nederland gevestigd is, gelden aanvullende wettelijke voorwaarden en dient een bewerkersovereenkomst op maat opgesteld te worden.
- Naast onvoldoende beveiliging kan onvoldoende transparantie van de kant van de bewerker ook leiden dat de verantwoordelijke niet voldoet aan zijn wettelijke

[4] zie hiervoor het document Inkoop voorwaarden en beveiligingseisen van de IBD en het in ontwikkeling zijnde GIBIT (KING)

verplichtingen. Aspecten die in dit kader beschreven dienen te worden zijn transparantie over de beveiliging en opgetreden beveiligingsincidenten. Maak hierbij afspraken over:
    - de inhoud en de frequentie van de rapportages die de bewerker aan de verantwoordelijke oplevert over de beveiliging; omschrijving van het recht van de verantwoordelijke om de naleving van de beveiligingsmaatregelen door onafhankelijke deskundigen vast te laten stellen.
    - de inhoud van rapportages over beveiligingsincidenten en datalekken, de criteria voor rapportage van incidenten en de snelheid waarmee wordt gerapporteerd. In de afspraken is opgenomen dat de bewerker beveiligingsincidenten en datalekken die (mogelijk) gevolgen hebben voor betrokkenen meteen rapporteert en dat de bewerker waar nodig ook meewerkt aan het adequaat informeren van de betrokkenen.
- 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 Third Party Memorandum (TPM), waarbij de verantwoordelijke de mogelijkheid van controle heeft.

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.

De Autoriteit Persoonsgegevens (AP)[6] biedt een aantal handreikingen ten behoeve van het opstellen van de bewerkersovereenkomst, zie hiervoor:

- De Beleidsregels (voorheen: Richtsnoeren) beveiliging van persoonsgegevens, paragraaf 4.2 en paragraaf 4.3: https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf

[5] Zie bijvoorbeeld: De Beleidsregels (Voorheen: Richtsnoeren) beveiliging van persoonsgegevens, paragraaf 4.2 en paragraaf 4.3 (https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf)
[6] Voorheen het College Bescherming Persoonsgegevens (CBP)

2 Model bewerkersovereenkomst

2.1 Algemeen

Dit model is een voorbeeld van een bewerkersovereenkomst. Uiteraard is het niet het enige mogelijke model en is het denkbaar dat overeenkomsten meer of andere bepalingen bevatten die eveneens aan de Wbp voldoen.

Deze modelovereenkomst bevat generieke bepalingen die betrekking hebben op het naleven van de Wbp door de bewerker. Zoals al is aangegeven moet u bij gebruik van het model bij de BRP bedacht zijn op de juiste verwijzigingen naar de BRP en moet u duidelijk maken dat het Besluit en de Regeling BRP altijd gelden en op onderdelen net iets specifieker is dan de Wbp of de model overeenkomst, bijvoorbeeld artikel 8 onder d. van het besluit basisregistratie personen over de verplichting tot opschorting.

Houdt u 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 dit model vervat zijn.

De bijlage bevat een selectie van BIG-maatregelen die onderwerp kunnen zijn van de bewerkersovereenkomst. De bijlage is een minimum variant en kan worden gezien als een startpunt en deze gaat uit van een generiek product of dienst zonder teveel achter de voordeur te kijken van de leverancier. De invulling en nadere specificatie is aan de gemeente zelf. Bij twijfel kan bijvoorbeeld ook een risicoanalyse worden uitgevoerd. De bijlage is gebaseerd op een minimale set op basis van SaaS dienstverlening. Voor IaaS en PaaS kunnen nog minder maatregelen geselecteerd worden omdat bij deze Cloudmodellen nog meer maatregelen bij de verantwoordelijke thuishoren en minder maatregelen bij de bewerker. Hetzelfde geldt als gebruik gemaakt wordt van een subbewerker (door een bewerker), deze zal waarschijnlijk weer minder maatregelen ontvangen als gevolg van het feit dat een subbewerker vaak maar een deel van wat de bewerker aanbiedt uitvoert.

2.2 Aansprakelijkheid

Over aansprakelijkheid (artikelen 10.1 tot en met 10.3 bewerkersovereenkomst) ontstaat vaak discussie en in dat verband is het belangrijk in te gaan op wat de Wbp daarover zegt in artikelen 49 en 50:

Artikel 49, derde lid, bepaalt dat de verantwoordelijke aansprakelijk is voor niet-naleving van de regels, door wie dan ook. Zou blijken dat de bewerker fouten heeft gemaakt dan kan de verantwoordelijke vervolgens de bewerker aanspreken. Daarnaast is de bewerker zelfstandig aansprakelijk voor eigen handelen. Beiden kunnen dus worden aangesproken door iemand die meent te zijn benadeeld bij de verwerking van zijn gegevens. Slechts wanneer verantwoordelijke of bewerker kunnen aantonen dat hun de schade niet kan worden aangerekend, gaan zij, blijkens het vierde lid, vrijuit.

De bepaling impliceert dus dat ook indien er een bewerker is die gegevens verwerkt ten behoeve van een verantwoordelijke, ook steeds die verantwoordelijke daarvoor aansprakelijk is. De

verwerking blijft immers altijd onder de verantwoordelijkheid van de verantwoordelijke plaatsvinden. Daarnaast is de bewerker ook zelfstandig aansprakelijke voor zijn aandeel in de schade.

Bovengenoemde bepalingen uit de wet zijn dwingend recht en afwijkende bepalingen in overeenkomsten ten nadele van de betrokkene zijn nietig.

De leverancier is in de praktijk verantwoordelijk voor het uitvoeren van de maatregelen die nodig zijn voor het beveiligen van ICT. Juist door het aansprakelijk stellen voor schade die ontstaat door gebrekkige beveiliging wordt de softwareleverancier verplicht om de geleverde programmatuur uitgebreid te testen op beveiligingslekken. Ook zou in een Service Level Agreement (SLA) kunnen worden afgesproken dat een ICT-dienstverlener waaraan de data van een organisatie wordt toevertrouwd de inspanning levert om deze zo goed mogelijk te beschermen. Met het accepteren van hieruit voortvloeiende aansprakelijkheid wordt een ICT-dienstverlener gedwongen om zich in te zetten voor het faciliteren van veilig ICT-gebruik.

De overeenkomst

Bewerkersovereenkomst van de gemeente <GEMEENTE> met de (nader in te vullen) bewerker

Het College van Burgemeester en Wethouders[7] van de gemeente <GEMEENTE>, verder te noemen de verantwoordelijke, ten deze rechtsgeldig vertegenwoordigd door de <heer of mevrouw> <persoonsnaam>.,

en

<Bedrijf, afdeling>, gevestigd te <plaatsnaam>, verder te noemen de bewerker, ten deze rechtsgeldig vertegenwoordigd door de <de heer of mevrouw>, <persoonsnaam> , <functie>,

verklaren te zijn overeengekomen een bewerkersovereenkomst als bedoeld in artikel 14, tweede lid, van de Wbp[8], tussen de verantwoordelijke en 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 standaarden 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<door gemeente bij te voegen>.

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.

[7] Bij gemeenten is het bevoegde bestuursorgaan de Wbp verantwoordelijke, in bijna alle gevallen is dat het College. Bij OOV en Koninklijke onderscheidingen is dat de Burgemeester.
[8] Bij gebruik voor de BRP moet u verwijzen naar art. 7 van het Besluit BRP.

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

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 bewerker als bewerker van persoonsgegevens optreedt in het kader van de door de verantwoordelijke ter beschikking gestelde persoonsgegevens voor <nader in te vullen omschreven doel>

Onderwerp van deze overeenkomst
Artikel 3.
3.1 De bewerker verwerkt persoonsgegevens in opdracht van de verantwoordelijke in het kader van de uitvoering van < contract, nummer>; dit is de onderliggende hoofdovereenkomst. De door de bewerker uit te voeren werkzaamheden waar deze bewerkersovereenkomst betrekking op heeft, worden nader omschreven in bijlage 1.
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 De bewerker neemt passende technische en organisatorische beveiligingsmaatregelen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Deze beveiligingsmaatregelen garanderen een passend beveiligingsniveau gelet op de te verrichten verwerkingen.

Naleving wet- en regelgeving
Artikel 4.
4.1 De Dienst / sector / cluster <afdelingsnaam> van de gemeente <GEMEENTE> treedt namens de verantwoordelijke op als contactpersoon.
4.2 De bewerker verwerkt gegevens ten behoeve van de verantwoordelijke, in overeenstemming met diens instructies.
4.3 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.
4.4 De bewerker zal bij de verwerking van persoonsgegevens in het kader van de in artikel 3 genoemde werkzaamheden, handelen in overeenstemming met de toepasselijke wet- en regelgeving betreffende de bescherming van persoonsgegevens. De bewerker verwerkt persoonsgegevens slechts in opdracht van de verantwoordelijke en zal alle redelijke instructies van de contactpersoon, als bedoeld in het eerste lid, dienaangaande opvolgen, behoudens afwijkende wettelijke verplichtingen.
4.5 De bewerker zal onmiddellijk bij het ontdekken van beveiligingsinbreuken of datalekken deze melden aan de verantwoordelijke, al dan niet onder verbeurte van een boete in geval van niet-nakoming, conform artikel 10.3 van deze overeenkomst.
4.6 De bewerker zal te allen tijde op eerste verzoek van de de contactpersoon, als bedoeld in het eerste lid, afkomstige persoonsgegevens met betrekking tot deze bewerkersovereenkomst ter hand stellen.
4.7 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.

4.8 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 de werkzaamheden als bewerker daartoe noodzaken. De medewerkers van de bewerker tekenen hiertoe een geheimhoudingsverklaring.

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 verantwoordelijke onmiddellijk, voorafgaand aan de verstrekking, ter zake informeren. Tenzij wettelijke bepalingen dit verbieden.

Meldplicht datalekken en beveiligingsincidenten

Artikel 6

6.1 De bewerker zal de verantwoordelijke zo spoedig mogelijk – doch uiterlijk binnen 24 uur na de eerste ontdekking – informeren over alle inbreuken op de beveiliging alsmede andere incidenten die op grond van wetgeving moeten worden gemeld aan een toezichthouder of betrokkene, onverminderd de verplichting de gevolgen van dergelijke inbreuken en incidenten zo snel mogelijk ongedaan te maken dan wel te beperken.

6.2 De bewerker zal het doen van meldingen aan de toezichthouder(s) overlaten aan de verantwoordelijke.

6.3 De bewerker zal alle noodzakelijke medewerking verlenen aan het zo nodig, op de kortst mogelijke termijn, verschaffen van aanvullende informatie aan de toezichthouder(s) en/of betrokkene(n).

6.4 De bewerker houdt een gedetailleerd logboek bij van alle inbreuken op de beveiliging, evenals de maatregelen die in vervolg op dergelijke inbreuken zijn genomen, en geeft daar op eerste verzoek van de verantwoordelijke inzage in.

Beveiligingsmaatregelen

Artikel 7.

7.1 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. De wijze van beveiliging wordt nader omschreven in bijlage 2.

7.2 De verantwoordelijke is te allen tijde gerechtigd de verwerking van persoonsgegevens te (doen) 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.

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

7.4 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.

7.5 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.

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

7.7 Naast rapportages door de bewerker en audits door de verantwoordelijke of controlerende instantie in opdracht van de verantwoordelijke, kunnen beide partijen ook overeenkomen gebruik te maken van een Third Party Memorandum (TPM) opgesteld door een onafhankelijke externe deskundige.

Inschakeling derden

Artikel 8.

8.1 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.

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

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

Wijziging overeenkomst

Artikel 9.

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

9.2 Zodra de samenwerking is beëindigd, zal de bewerker naar keuze van de verantwoordelijke (i) alle of een door verantwoordelijke bepaald gedeelte van haar in het kader van deze overeenkomst ter beschikking gestelde persoonsgegevens aan de verantwoordelijke ter beschikking stellen (ii) de persoonsgegevens die hij van de verantwoordelijke heeft ontvangen op alle locaties vernietigen, in welke vorm dan ook en toont dit aan, tenzij partijen iets anders overeenkomen. De verantwoordelijk kan zo nodig nadere eisen stellen aan de wijze van beschikbaarstelling, waaronder eisen aan het bestandsformaat, dan wel vernietiging. Deze werkzaamheden moeten, binnen nader overeen te komen termijn, uitgevoerd worden en hiervan wordt een verslag gemaakt.

9.3 De bewerker zal te allen tijde de in het vorig lid beschreven dataportabiliteit waarborgen zodanig dat er geen sprake is van verlies van functionaliteit of (delen van) de gegevens.

9.3 Elk van de partijen is gerechtigd de overeenkomst met onmiddellijke ingang te beëindigen bij een zodanige wijziging van wettelijke regels dat een verdere voortzetting van de overeenkomst niet kan worden verlangd.

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

9.5 Verantwoordelijke en bewerker treden met elkaar in overleg over wijzigingen in deze overeenkomst als een wijziging in regelgeving of een wijziging in de uitleg van regelgeving daartoe aanleiding geven.

Aansprakelijkheid

Artikel 10.

10.1 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.

10.2 Bewerker is aansprakelijk op grond van het bepaalde in artikel 49 van de Wbp, schade of nadeel voortvloeiende uit het niet nakomen van deze overeenkomst daaronder begrepen.

10.3. Bewerker vrijwaart Verantwoordelijke voor schade of nadeel voor zover ontstaan door werkzaamheid van de Bewerker.

Toepasselijk recht

Artikel 11.

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

Citeertitel

Artikel 12.

12.1 Deze overeenkomst kan worden aangehaald als 'Bewerkersovereenkomst uitvoering <……>'.

Aldus in tweevoud opgesteld en getekend de dato

Namens de verantwoordelijke, de Dienst / Afdeling / cluster <afdelingsnaam> van de gemeente <GEMEENTE>,

de

Namens de <nader in te vullen gegevens bewerker>
<nader in te vullen gegevens vertegenwoordiger bewerker, zoals genoemd in de aanhef>

Bijlage 1: omschrijving werkzaamheden ter uitwerking van artikel 3

1. De werkzaamheden van de bewerker (de verleende diensten en de bijbehorende verwerking).

Hier een lijstje opnemen met werkzaamheden die veel voorkomen zoals:

- Hosting bestaande uit activiteiten zoals…
- Back-ups maken en restoren
- Applicatiebeheer bestaande uit activiteiten zoals…
- Technisch beheer bestaande uit activiteiten zoals…
- Database beheer bestaande uit activiteiten zoals…
- Helpdesk bestaande uit activiteiten zoals…
- Communicatievoorziening (zoals berichtenverkeer)
- Archiefbeheer
- Vernietiging van gegevensdragers
- Printing, scanning, kopieren (lease van Multifunctionals)
- Inhoudelijke werkzaamheden die namens de gemeente worden uitgevoerd zoals:
    - Uitgifte parkeervergunningen
    - Voeren salarisadministratie
    - Bijvoorbeeld: uitvoeren bepaalde gemeentelijke taken uit de Jeugdwet, WMO, participatiewet

Indien de werkzaamheden in de hoofdovereenkomst specifiek omschreven zijn, kan dit lijstje achterwege blijven. Of hier verwijzen naar de hoofdovereenkomst. De achtergond van de beschrijving is dat je voldoende duidelijk maakt wat er beveiligd moet worden. Het is de bedoeling dat de zinnen afgemaakt worden met specifieke omschrijvingen!

2. Omschrijving van de werkzaamheden van de derden (subbewerkers) als deze er zijn, als bedoeld in artikel 8.

Lijstje opnemen met werkzaamheden die veel voorkomen zoals:

- Hosting bestaande uit activiteiten zoals…
- Back-ups maken en restoren
- Applicatiebeheer bestaande uit activiteiten zoals…
- Technisch beheer bestaande uit activiteiten zoals…
- Database beheer bestaande uit activiteiten zoals…
- Helpdesk bestaande uit activiteiten zoals…
- Communicatievoorziening (zoals berichtenverkeer)
- Onderhoud aan multifunctionals

De achtergond van de beschrijving is dat er voldoende duidelijk gemaakt wordt wat er beveiligd moet worden. Ook hier geldt dat de zinnen afgemaakt worden met specifieke omschrijvingen!

3. Categorieën personen en soorten persoonsgegevens

Algemene omschrijving van de categorien personen waar de gegevens die verwerkt worden betrekking op hebben zoals: personeelsleden, burgers, inschrevenen, vergunning aanvragers, voorziening aanvragers (clienten).
Is er bij de verwerkte gegevens sprake van gegevens van gevoelige aard als bedoelt in de beleidsregels datalekken van de AP:

- Bijzondere persoonsgegevens zoals bedoeld in artikel 16 Wbp. Het gaat hierbij om persoonsgegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en om strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag. Het BSN valt ook onder bijzondere persoonsgegevens.
- Gegevens over de financiële of economische situatie van de betrokkene. Hieronder vallen bijvoorbeeld gegevens over (problematische) schulden, salaris- en betalingsgegevens.
- (Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene. Hieronder vallen bijvoorbeeld gegevens over gokverslaving, prestaties op school of werk of relatieproblemen.
- Gebruikersnamen, wachtwoorden en andere inloggegevens. De mogelijke gevolgen voor betrokkenen hangen af van de verwerkingen en van de persoonsgegevens waar de inloggegevens toegang toe geven. Bij de afweging moet worden betrokken dat veel mensen wachtwoorden hergebruiken voor verschillende verwerkingen.
- Gegevens die kunnen worden misbruikt voor (identiteits)fraude. Het gaat hierbij onder meer om biometrische gegevens, kopieën van identiteitsbewijzen en om het Burgerservicenummer (bsn).

Is er sprake van de verwerking van gegevens over kwetsbare groepen zoals:

- minderjarigen;
- mensen die te maken hebben met stalking;
- die in een blijf-van-mijn-lijfhuis verblijven.

Voor bepaalde categorieën van betrokkenen:

- kinderen en mensen met een verstandelijke handicap.

Bijlage 2: Beschrijving beveiliging ter uitwerking van artikel 7 lid 1

1. Normenstelsel (kies a of b)
   a. De informatiebeveiliging vindt plaats volgens algemeen erkende normen, namelijk: *(vermeld normenstelsel, zoals bijvoorbeeld NEN7510, NEN/ISO 27001, PCI/DSS)*
   b. De informatiebeveiliging vindt plaats volgens een algemeen erkende overheidsnorm zoals de BIG of de BIR of vergelijkbaar.
2. De toereikendheid van de informatiebeveiliging blijkt uit:
   a. Certificering;
   b. Periodieke externe controles zoals audits of TPM's (bijv. ISAE3xxx SOC type II);
   c. Een Assurance rapport met conclusie over de bevindingen van de auditor;
   d. Eigen controles of eigen mededelingen.
3. Uit de certificering of periodieke externe controles of uit de audits of uit de eigen controles blijkt of kan afgeleid worden dat de beveiliging voldoet aan of gelijkwaardig is met de toelichting (bijlage 3) en de daarin omschreven elementen.
   LET OP: gemotiveerd afwijken is toegestaan!

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

INFORMATIE
BEVEILIGINGS
DIENST

Bijlage 3: Toelichting: Maatregelen op basis van de BIG ten aanzien van een bewerker

Deze bijlage is gevuld met een suggestie van gekozen maatregelen uit de BIG en kunnen ook worden uitgebreid of aangepast. Nadruk ligt op de integriteit en exclusiviteit van de gegevens, beschikbaarheidseisen horen bij voorkeur in een SLA thuis.

Deze maatregelen zijn uit de BIG afkomstig en waar mogelijk specifiek gemaakt voor de bewerker. Deze maatregelen gaan uit van het niveau van de BIG. Als de gegevens van de verantwoordelijke hoger geclassificeerd zijn, een hogere risico inschatting hebben (bijzondere persoonsgegevens) of extra maatregelen nodig hebben uit specifieke wetgeving, dan dient deze bijlage te worden uitgebreid.

BIG Nummer	titel	Maatregel bewerker	SaaS	PaaS	IaaS	Applicatie beheer	Technisch/ database beheer	Helpdesk	Berichten verkeer	Archief beheer	Vernietiging van gegevensdra	Lease MFP	Inhoudelijk proces
6.1.5.1	Geheimhoudingsovereenkomst	Medewerkers die te maken hebben met persoonsinformatie van de verantwoordelijke dienen een geheimhoudingsverklaring te ondertekenen. Hierbij wordt tevens vastgelegd dat na beëindiging van de functie, de betreffende persoon gehouden blijft aan die geheimhouding.	x	x		x	x	x	x	x	x	x	x
6.1.8.2	Onafhankelijke beoordeling van informatiebeveiliging	Periodieke beveiligingsaudits (minimaal eens per twee jaar) worden uitgevoerd volgens afspraken met de verantwoordelijke.	x	x		x	x	x	x	x	x	x	x
6.2.1.7	Identificatie van risico's die betrekking hebben op externe partijen	Over het naleven van de afspraken wordt jaarlijks gerapporteerd aan de verantwoordelijke.	x	x	x	x	x	x	x	x	x	x	x

BIG Nummer	titel	Maatregel bewerker	SaaS	PaaS	IaaS	Applicatie beheer	Technisch/ database beheer	Helpdesk	Berichten verkeer	Archief beheer	Vernietiging van gegevensdra	Lease MFP	Inhoudelijk proces
6.2.3.1	Beveiliging behandelen in overeenkomsten met een derde partij	Maatregelen uit de bewerkersovereenkomst zijn geïmplementeerd.	x	x	x	x	x	x	x	x	x	x	X
7.2.2.1	Labeling en verwerking van informatie	De bewerker heeft maatregelen genomen zo dat niet geautoriseerden geen kennis kunnen nemen van persoonsgegevens.	x			x	x	x	x	x	x	x	X
8.1.1.2	Rollen en verantwoordelijkheden	Het personeel van de bewerker of derden moeten kennis hebben van de verantwoordelijkheden ten aanzien van de bewerking van de persoonsgegevens voor de verantwoordelijke.	x			x	x	x	x	x	x	x	x
8.1.2.1	Screening	Voor personen is een recente Verklaring Omtrent het Gedrag (VOG) vereist met punten die door de verantwoordelijke zijn aangedragen. Tenzij dit centraal in het contract geregeld is.	x			x	x	x	x	x	X	x	X
8.3.3.1	Blokkering van toegangsrechten	Toegangsrechten van medewerkers van de bewerker worden direct geblokkeerd als geen toegang voor de bewerking van de persoonsgegevens noodzakelijk is.	x			x	x	x	x	x	X	x	x

BIG Nummer	titel	Maatregel bewerker	SaaS	PaaS	IaaS	Applicatie beheer	Technisch/ database beheer	Helpdesk	Berichten verkeer	Archief beheer	Vernietiging van gegevensdra	Lease MFP	Inhoudelijk proces
9.1.2.1	Fysieke toegangsbeveiliging	Toegang tot beveiligde zones of gebouwen waar persoonsgegevens van de verantwoordelijke zich bevinden is alleen mogelijk na autorisatie daartoe.	x	x	x	x	x	x	x	x	x	x	x
9.1.3.1	Beveiliging van kantoren, ruimten en faciliteiten	Papieren documenten en mobiele gegevensdragers die persoonsgegevens of andere vertrouwelijke gegevens van de verantwoordelijke bevatten worden beveiligd opgeslagen.	x			x	x	x	x	x	x	x	x
10.3.1.1	Capaciteitsbeheer	De ICT-voorzieningen voldoen aan het voor de dienst overeengekomen niveau van beschikbaarheid. Er worden voorzieningen geïmplementeerd om de beschikbaarheid van componenten te bewaken (bijvoorbeeld de controle op aanwezigheid van een component en metingen die het gebruik van een component vaststellen). Op basis van voorspellingen van het gebruik wordt actie genomen om tijdig de benodigde uitbreiding van capaciteit te bewerkstelligen. Op basis van een risicoanalyse wordt bepaald wat de beschikbaarheidseis van een ICT-voorziening is en wat de impact bij uitval is. Afhankelijk daarvan worden maatregelen bepaald zoals automatisch werkende mechanismen om uitval van (fysieke) ICT-voorzieningen,	x	x	x	x	x	x	x	x	x	x	x

BIG Nummer	titel	Maatregel bewerker	SaaS	PaaS	IaaS	Applicatie beheer	Technisch/ database beheer	Helpdesk	Berichten verkeer	Archief beheer	Vernietiging van gegevensdra	Lease MFP	Inhoudelijk proces
		waaronder verbindingen op te vangen.											
10.6.1.2	Maatregelen voor netwerken	Gegevensuitwisseling tussen vertrouwde en niet vertrouwde zones dient inhoudelijk geautomatiseerd gecontroleerd te worden op aanwezigheid van malware.	x	x			x	x	x			x	x
10.6.1.3	Maatregelen voor netwerken	Bij transport van vertrouwelijke informatie over niet vertrouwde netwerken tussen de bewerker en de verantwoordelijke, zoals over het internet, dient altijd geschikte encryptie te worden toegepast. Zie hiertoe 12.3.1.3.	x	x			x	x	x			x	x
10.6.2.1	Beveiliging van netwerkdiensten	Beveiligingskenmerken, niveaus van dienstverlening en beheer eisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in elke overeenkomst voor netwerkdiensten, zowel voor diensten die intern worden geleverd als voor uitbestede diensten door een bewerker.	x				x	x	x			x	x
10.8.2.2	Uitwisselingsovereenkomsten	Verantwoordelijkheid en aansprakelijkheid in het geval van informatiebeveiligingsincidenten zijn beschreven, evenals procedures over melding van incidenten van de bewerker naar de verantwoordelijke.	x			x	x	x	x	x	x	x	x

BIG Nummer	titel	Maatregel bewerker	SaaS	PaaS	IaaS	Applicatie beheer	Technisch/ database beheer	Helpdesk	Berichten verkeer	Archief beheer	Vernietiging van gegevensdra	Lease MFP	Inhoudelijk proces
10.8.3.1	Fysieke media die worden getransporteerd	De bewerker neemt maatregelen om vertrouwelijke informatie te beschermen, zoals: • Versleuteling. • Bescherming door fysieke maatregelen, zoals afgesloten containers. • Gebruik van verpakkingsmateriaal waaraan te zien is of getracht is het te openen • Persoonlijke aflevering. • Opsplitsing van zendingen in meerdere delen en eventueel verzending via verschillende routes.	x						x	x	x		x
10.10.1.1	Aanmaken auditlogbestanden	Door de bewerker worden rapportages van logbestanden gemaakt die periodiek worden beoordeeld. Deze periode dient te worden gerelateerd aan de mogelijkheid van misbruik en de schade die kan optreden.	x	x		x	x		x		x		X
10.10.1.2	Aanmaken auditlogbestanden	Een logregel bevat minimaal: • Een tot een natuurlijk persoon herleidbare gebruikersnaam of ID. • De gebeurtenis (zie 10.10.2.1). • Waar mogelijk de identiteit van het werkstation of de locatie. • Het object waarop de handeling werd uitgevoerd. • Het resultaat van de handeling. • De datum en het tijdstip van de gebeurtenis.	x			x	x		x	x	x	x	x

BIG Nummer	titel	Maatregel bewerker	SaaS	PaaS	IaaS	Applicatie beheer	Technisch/ database beheer	Helpdesk	Berichten verkeer	Archief beheer	Vernietiging van gegevensdra	Lease MFP	Inhoudelijk proces
10.10.1.3	Aanmaken auditlogbestanden	In een logregel wordt in geen geval gevoelige gegevens opgenomen. Dit betreft onder meer gegevens waarmee de beveiliging doorbroken kan worden (zoals wachtwoorden, inbelnummers, et cetera).	x			x	x		x	x	x	x	x
10.10.2.1	Controle van systeemgebruik	De volgende gebeurtenissen worden in ieder geval opgenomen in de logging: • Gebruik van technische beheerfuncties, zoals het wijzigingen van configuratie of instelling: uitvoeren van een systeemcommando, starten en stoppen, uitvoering van een back-up of restore. • Gebruik van functioneel beheerfuncties, zoals het wijzigingen van configuratie en instellingen, release van nieuwe functionaliteit, ingrepen in gegevenssets (waaronder databases). • Handelingen van beveiligingsbeheer, zoals het opvoeren en afvoeren gebruikers, toekennen en intrekken van rechten, wachtwoord reset, uitgifte en intrekken van cryptosleutels. • Beveiligingsincidenten (zoals de aanwezigheid van malware, testen op vulnerabilities, foutieve inlogpogingen, overschrijding van autorisatiebevoegdheden, geweigerde pogingen om toegang te	x	x		x	x		x	x	x	x	x

BIG Nummer	titel	Maatregel bewerker	SaaS	PaaS	IaaS	Applicatie beheer	Technisch/ database beheer	Helpdesk	Berichten verkeer	Archief beheer	Vernietiging van gegevensdra	Lease MFP	Inhoudelijk proces
		krijgen, het gebruik van niet operationele systeemservices, het starten en stoppen van security services). • Verstoringen in het productieproces (zoals het vollopen van queues, systeemfouten, afbreken tijdens executie van programmatuur, het niet beschikbaar zijn van aangeroepen programmaonderdelen of systemen). • Handelingen van gebruikers, zoals goede en foute inlogpogingen, systeemtoegang, gebruik van online transacties en toegang tot bestanden door systeembeheerders.											
10.10.3.3	Bescherming van informatie in logestanden	Logbestanden worden zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden.	x	x		x	x		x	x	x	x	x
10.10.3.5	Bescherming van informatie in logestanden	De beschikbaarheid van loginformatie is gewaarborgd binnen de termijn waarin loganalyse noodzakelijk wordt geacht, met een minimum van drie maanden, conform de wensen van de verantwoordelijke. Bij een (vermoed) informatiebeveiligingsincident is de bewaartermijn minimaal drie jaar.	x	x									

BIG Nummer	titel	Maatregel bewerker	SaaS	PaaS	IaaS	Applicatie beheer	Technisch/ database beheer	Helpdesk	Berichten verkeer	Archief beheer	Vernietiging van gegevensdra	Lease MFP	Inhoudelijk proces
10.10.6.1	Synchronisatie van systeemklokken	Er worden maatregelen genomen om er voor te zorgen dat de logbestanden die verzameld worden aan elkaar te relateren zijn, op basis van het tijdstip waarin ze zijn opgetreden.	x	x	x	x	x		x	x	x	x	x
11.4.2.1	Authenticatie van gebruikers bij externe verbindingen.	Als externe toegang nodig is tot de persoonsgegevens van de verantwoordelijke door eigen personeel, of personeel van de bewerker, dienen geschikte authenticatie methodes te worden gebruikt.	x			x	x	x	x	x	x	x	x
11.4.5.5	Scheiding van netwerken	Zonering wordt ingericht met voorzieningen waarvan de functionaliteit is beperkt tot het strikt noodzakelijke (hardening van voorzieningen).	x			x	x	x	x	x		x	x
11.5.1.1	Beveiligde inlogprocedures	Toegang tot de persoonsgegevens van de verantwoordelijke wordt verleend op basis van twee-factor authenticatie.				x	x	x	x	x	x	x	x
11.5.1.2	Beveiligde inlogprocedures	Het wachtwoord wordt niet getoond op het scherm tijdens het ingeven. Er wordt geen informatie getoond die herleidbaar is tot de authenticatiegegevens.	x			x	x	x	x	x		x	X
11.5.1.3	Beveiligde inlogprocedures	Voorafgaand aan het aanmelden wordt aan de gebruiker een melding getoond dat alleen geautoriseerd gebruik is toegestaan voor expliciet door de organisatie vastgestelde doeleinden.	x			x	x	x					x

BIG Nummer	titel	Maatregel bewerker	SaaS	PaaS	IaaS	Applicatie beheer	Technisch/ database beheer	Helpdesk	Berichten verkeer	Archief beheer	Vernietiging van gegevensdra	Lease MFP	Inhoudelijk proces
11.5.1.4	Beveiligde inlogprocedures	Bij een succesvol loginproces wordt de datum en tijd van de voorgaande login of loginpoging getoond. Deze informatie kan de gebruiker enige informatie verschaffen over de authenticiteit en/of misbruik van het systeem.	x			x	x	x					X
11.5.1.5	Beveiligde inlogprocedures	Nadat voor een gebruikersnaam 3 keer een foutief wachtwoord gegeven is, wordt het account minimaal 10 minuten geblokkeerd. Indien er geen lock-out periode ingesteld kan worden, dan wordt het account geblokkeerd totdat de gebruiker verzoekt deze lock-out op te heffen of het wachtwoord te resetten.	x			x	x	x					X
11.5.2.1	Gebruikersidentificatie en -authenticatie	Bij uitgifte van authenticatiemiddelen wordt minimaal de identiteit vastgesteld, evenals het feit dat de gebruiker recht heeft op het authenticatiemiddel.	x			x	x	x					X
11.5.3.1	Systemen voor wachtwoordbeheer	Er wordt automatisch gecontroleerd op goed gebruik van wachtwoorden (onder andere voldoende sterke wachtwoorden, regelmatige wijziging, directe wijziging van initieel wachtwoord).	x			x	x	x					X
11.5.5.1	Time-out van sessies	De periode van inactiviteit van een werkstation is vastgesteld op maximaal 15 minuten. Daarna wordt de PC vergrendeld. Bij remote desktop sessies geldt dat na maximaal 15 minuten inactiviteit de	x			x	x	x					X

BIG Nummer	titel	Maatregel bewerker	SaaS	PaaS	IaaS	Applicatie beheer	Technisch/ database beheer	Helpdesk	Berichten verkeer	Archief beheer	Vernietiging van gegevensdra	Lease MFP	Inhoudelijk proces
		sessie verbroken wordt.											
11.5.6.1	Beperking van verbindingstijd	De toegang voor onderhoud op afstand door een leverancier wordt alleen opengesteld op basis van een wijzigingsverzoek of storingsmelding, met 2-factor authenticatie en tunneling.	x			X	x	x		x		x	x
11.6.1.1	Beperking van toegang tot informatie	In de soort toegangsregels wordt ten minste onderscheid gemaakt tussen lees- en schrijfbevoegdheden.	x			x	x	x				x	x
11.6.1.2	Beperking van toegang tot informatie	Managementsoftware heeft de mogelijkheid gebruikerssessies af te sluiten.	x			x	x	x					x
11.6.1.3	Beperking van toegang tot informatie	Bij extern gebruik vanuit een niet vertrouwde omgeving vindt sterke authenticatie (two-factor) van gebruikers plaats.	x			x	x	x		x			x
12.1.1.1	Analyse en specificatie van beveiligingseis en	In projecten ten behoeve van systemen voor de verantwoordelijke wordt een beveiligingsrisicoanalyse en maatregelbepaling opgenomen als onderdeel van het ontwerp. Ook bij wijzigingen worden de veiligheidsconsequenties meegenomen.	x			x	x			x			x

BIG Nummer	titel	Maatregel bewerker	SaaS	PaaS	IaaS	Applicatie beheer	Technisch/ database beheer	Helpdesk	Berichten verkeer	Archief beheer	Vernietiging van gegevensdra	Lease MFP	Inhoudelijk proces
12.2.1.1	Validatie van invoergegevens	Er moeten controles worden uitgevoerd op de invoer van gegevens. Daarbij wordt minimaal gecontroleerd op grenswaarden, ongeldige tekens, onvolledige gegevens, gegevens die niet aan het juiste format voldoen, toevoegen van parameters (SQL-Injectie) en inconsistentie van gegevens.	x			x	x		x				x
12.2.2.1	Beheersing van interne gegevensverwerking	Er bestaan voldoende mogelijkheden om reeds ingevoerde gegevens te kunnen corrigeren door er gegevens aan te kunnen toevoegen.	x			x	x		x				x
12.2.3.1	Integriteit van berichten	Er behoren eisen en geschikte beheersmaatregelen te worden vastgesteld en geïmplementeerd, voor het bewerkstelligen van authenticiteit en het beschermen van integriteit van berichten in toepassingen.	x	x		x	x	x	x	x	x	x	x
12.2.4.1	Validatie van uitvoergegevens	De uitvoerfuncties van programma's maken het mogelijk om de volledigheid en juistheid van de gegevens te kunnen vaststellen (bijvoorbeeld door check-sums).	x			x	x	x	x	x	x	x	X
12.3.1.1	Beleid voor het gebruik van cryptografische beheersmaatregelen	De gebruikte cryptografische algoritmen voor versleuteling zijn als open standaard gedocumenteerd en zijn door onafhankelijke betrouwbare deskundigen getoetst.	x	x		X	X	x	x	x	X	x	X

BIG Nummer	titel	Maatregel bewerker	SaaS	PaaS	IaaS	Applicatie beheer	Technisch/ database beheer	Helpdesk	Berichten verkeer	Archief beheer	Vernietiging van gegevensdra	Lease MFP	Inhoudelijk proces
12.3.2.1	Sleutelbeheer	In het sleutelbeheer is minimaal aandacht besteed aan het proces, de actoren en hun verantwoordelijkheden.	x	x		X	X	x	x	X	x	X	X
12.4.1.1	Beheersing van operationele software	Alleen geautoriseerd personeel kan functies en software installeren of activeren.	x	x		X	X	x	x	x	X	X	X
12.5.1.1	Procedures voor wijzigingsbeheer	Er is aantoonbaar wijzigingsmanagement ingericht volgens gangbare best practices, zoals ITIL en voor applicaties ASL.	x	x		x	X	x	x	x	X	X	x
12.5.2.1	Technische beoordeling van toepassingen na wijzigingen in het besturingssysteem	Van aanpassingen (zoals updates) aan softwarematige componenten van de technische infrastructuur wordt vastgesteld dat deze de juiste werking van de technische componenten niet in gevaar brengen en de beveiliging zoals afgesproken met de verantwoordelijke te niet doen.	x	x		x	x	x	x	x	x	x	
12.5.4.1	Uitlekken van informatie	Op het grensvlak van een vertrouwde en een niet vertrouwde omgeving vindt content-scanning plaats.	x	x	x	X	x	x	x	x	x	x	x
12.5.4.2	Uitlekken van informatie	Er dient een proces te zijn om aan de verantwoordelijke te melden dat (persoons) informatie is uitgelekt. (zie 13.1.1)	x	x	x	X	X	x	x	x	x	x	x

BIG Nummer	titel	Maatregel bewerker	SaaS	PaaS	IaaS	Applicatie beheer	Technisch/ database beheer	Helpdesk	Berichten verkeer	Archief beheer	Vernietiging van gegevensdra	Lease MFP	Inhoudelijk proces
12.6.1.1	Beheersing van technische kwetsbaarheden	Er is een proces ingericht voor het beheer van technische kwetsbaarheden. Dit omvat minimaal het melden van incidenten aan de verantwoordelijke, het uitvoeren van periodieke penetratietests, het uitvoeren van risicoanalyses van kwetsbaarheden en patching van systemen en hardware.	x	x	x	x	X	x	x	x	x	x	x
13.1.1.1	Rapportage van informatiebeveiligingsgebeurtenissen	Er is een procedure voor het rapporteren van beveiligingsgebeurtenissen aan de verantwoordelijke vastgesteld, in combinatie met een reactie- en escalatieprocedure voor incidenten, waarin de handelingen worden vastgelegd die moeten worden genomen na het ontvangen van een rapport van een beveiligingsincident.	x	x	x	X	X	x	x	x	x	x	x
13.1.1.4	Rapportage van informatiebeveiligingsgebeurtenissen	Alle beveiligingsincidenten worden vastgelegd in een systeem en geëscaleerd aan de verantwoordelijke.	x	x	x	X	X	x	x	x	x	x	x
13.1.1.5	Rapportage van informatiebeveiligingsgebeurtenissen	Vermissing of diefstal van apparatuur of media die gegevens van de verantwoordelijke kunnen bevatten wordt altijd ook aangemerkt als informatiebeveiligingsincident.	x	x	x	X	X	x	x	x	x	X	x

BIG Nummer	titel	Maatregel bewerker	SaaS	PaaS	IaaS	Applicatie beheer	Technisch/ database beheer	Helpdesk	Berichten verkeer	Archief beheer	Vernietiging van gegevensdra	Lease MFP	Inhoudelijk proces
13.2.3.1	Verzamelen van bewijsmateriaal	Voor een vervolgprocedure naar aanleiding van een beveiligingsincident behoort bewijsmateriaal te worden verzameld, bewaard en gepresenteerd in overeenstemming met de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.	x	x	x	x	x	x	x	x	x	X	x
15.1.3.1	Bescherming van bedrijfsdocumenten	De registraties van de verantwoordelijke behoren te worden beschermd tegen verlies, vernietiging en vervalsing, in overeenstemming met wettelijke en regelgevende eisen, contractuele verplichtingen en bedrijfsmatige eisen.	x			x	x			x			X
15.1.4.1	Bescherming van gegevens en geheimhouding van persoonsgegevens	De bescherming van gegevens en privacy behoort te worden bewerkstelligd in overeenstemming met relevante wetgeving, voorschriften en indien van toepassing contractuele bepalingen.	x			X	x			x			X
15.1.6.1	Voorschriften voor het gebruik van cryptografische beheersmaatregelen	Er is vastgesteld aan welke overeenkomsten, wetten en voorschriften de toepassing van cryptografische technieken moet voldoen. Zie ook 12.3.	x			x	x			x			X

BIG Nummer	titel	Maatregel bewerker	SaaS	PaaS	IaaS	Applicatie beheer	Technisch/ database beheer	Helpdesk	Berichten verkeer	Archief beheer	Vernietiging van gegevensdra	Lease MFP	Inhoudelijk proces
15.2.1.1	Naleving van beveiligingsbeleid en -normen	De bewerker is verantwoordelijk voor uitvoering en beveiligingsprocedures en toetsing daarop (onder andere de jaarlijkse in control verklaring). Conform deze bewerkersovereenkomst en andere contractuele eisen zorgt de bewerker voor het toezicht op de uitvoering van het beveiligingsbeleid ten behoeve van de gegevens van de verantwoordelijke. Daarbij behoren ook periodieke beveiligingsaudits. Deze kunnen worden uitgevoerd door, of vanwege de verantwoordelijke.	x	x		X	x	x	x	x	x	X	x
15.2.2.1	Controle op technische naleving	Informatiesystemen van de bewerker ten behoeve van de verantwoordelijke worden regelmatig gecontroleerd op naleving van beveiligingsnormen. Dit kan door bijvoorbeeld kwetsbaarheidsanalyses en penetratietesten.	x	x		x	x	x	x	x	x	x	x

INFORMATIE BEVEILIGINGS DIENST

**INFORMATIEBEVEILIGINGSDIENST
V00R GEMEENTEN (IBD)**

**NASSAULAAN 12
2514 JS DEN HAAG**

**POSTBUS 30435
2500 GK DEN HAAG**

HELPDESK 070 373 80 11

**INFO@IBDGEMEENTEN.NL
WWW.IBDGEMEENTEN.NL**

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN **IN OPDRACHT VAN**
VERENIGING VAN NEDERLANDSE GEMEENTEN