Baseline Bescherming Persoonsgegevens

Inleiding

Per 1 mei 2020 is voor de gemeenten Alphen aan den Rijn, Kaag en Braassem, Nieuwkoop en Waddinxveen een interne functionaris gegevensbescherming (FG) aangewezen. Naar rato van het aantal uren dat de FG besteedt per gemeente worden de respectievelijke kosten berekend. Synergievoordelen liggen echter niet alleen op het kostenvlak maar ook op inhoudelijk gebied. Uiteraard is samenwerking altijd bij uitstek een mogelijkheid om van elkaar te leren, maar de FG kan op het gebied van de bescherming van persoonsgegevens de gemeenten dichter bij elkaar brengen door bijvoorbeeld het opstellen van FG-aanwijzingen en door (meer) uniformiteit in rapportages en overlegvormen aan te brengen.

Normenkader

Een andere wijze voor het verkrijgen van meer uniformiteit is het hanteren van een gemeenschappelijk normenkader waarlangs de Rijnstreek gemeenten en de gemeente Waddinxveen door de functionaris gegevensbescherming worden getoetst op naleving van de Algemene Verordening Gegevensbescherming (AVG). Dit normenkader is de *Baseline Bescherming Persoonsgegevens*.

Doel

In deze Baseline Bescherming Persoonsgegevens zijn de eisen van de AVG en de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG) vertaald naar concrete, hanteerbare normen die duidelijk maken wat de vier gemeenten moeten doen om in overeenstemming met de wet de bescherming van persoonsgegevens van de betrokkenen te *waarborgen*. Door het toepassen van de Baseline kunnen de gemeenten tevens *aantonen* dat passende waarborgen voor de bescherming van persoonsgegevens worden getroffen. Als laatste doel heeft de Baseline het bewerkstelligen van meer uniformiteit in beleid en uitvoering.

Kwaliteit

Het centrale uitgangspunt van de AVG is dat persoonsgegevens slechts mogen worden verwerkt als er een wettelijke grondslag bestaat én het doel van de verwerking redelijkerwijs niet op een andere (minder ingrijpende) wijze kan worden verwezenlijkt. Dit houdt in dat persoonsgegevens alleen verwerkt mogen worden als de gegevens noodzakelijk zijn om het beoogde doel te bereiken.

De gemeenten kunnen er altijd voor kiezen om slechts te voldoen aan de minimale eisen die de wet stelt. Maar door weloverwogen en doelmatig om te gaan met de bescherming van persoonsgegevens en de balans te vinden tussen wetgeving, doelstellingen van de gemeente en respect voor de persoonlijke levenssfeer van burgers, medewerkers en andere

betrokkenen, is de bescherming van persoonsgegevens ook als een kwaliteitskenmerk van een gemeente te beschouwen.

Parameters
Deze Baseline bevat zeventien parameters waarlangs elke gemeente de bescherming van persoonsgegevens kan vormgeven overeenkomstig de eisen van de AVG. Per parameter wordt aangegeven hoe elke norm concreet ingevuld kan worden, wat het doel van de norm is en welke risico de gemeente loopt indien de norm niet of onvoldoende wordt ingevuld.

Toetsing
Op basis van de mate van invulling van de parameters zal de FG kunnen toetsten in hoeverre elke gemeente passende maatregelen en waarborgen treft ter bescherming van persoonsgegevens en in hoeverre de gemeente dat ook kan aantonen.

Groeimodel
Natuurlijk is het onredelijk om onmiddellijk van de gemeenten een volmaakte naleving van de eisen uit de AVG te verwachten. Wellicht is deze toestand ook onbereikbaar. Maar dat gezegd hebbende, ontslaat dat de gemeente niet van de verplichting te streven naar continue verbetering. De Baseline moet daarom ook worden gezien als een groeimodel, waarbinnen elke gemeente zelf haar ambitie en volwassenheidsniveau kan bepalen.

Parameters

Parameter 1: Visie

Het duidelijk voor ogen hebben van een visie op de bescherming van persoonsgegevens is essentieel voor de inbedding, vooruitgang en ontwikkeling van dit onderwerp binnen de gemeente. Een visie geeft richting en verwoordt de ambitie van de gemeente op het gebied van de bescherming van persoonsgegevens.

Concreet	Het visualiseren en documenteren van een gewenste situatie over vijf jaar op het gebied van de bescherming van persoonsgegevens waarbij zoveel mogelijk relevante partijen betrokken worden.
Doel	Het hebben van richting waarlangs de gemeente op basis van haar ambitie een gewenste toekomstige situatie kan bereiken.
Risico	Door gebrek aan visie is er een zwalkend beleid en wordt telkens opnieuw het wiel uitgevonden.

Parameter 2: Doelen en strategie

Uit de ontwikkelde visie worden de doelen afgeleid. Het bereiken van deze doelen leidt tot het realiseren van de visie. De manier waarop de volgorde van de doelen bepaald wordt en

de aanpak die leidt tot het bereiken van de doelen is de strategie. De doelen moeten specifiek, meetbaar, aanvaardbaar, realistisch en tijdgebonden omschreven worden.

Concreet	Door het opdelen van de visie in hapklare brokken worden de doelen bepaald. Het in lijn brengen en in de tijd wegzetten van deze doelen aan de hand van een uiteenzetting van de aanpak is de strategie. SMART-indicatoren worden opgesteld om te kunnen bepalen of aanpak nog op koers ligt en of de doelen bereikt zijn.
Doel	Per jaar omschrijven welke doelen behaald moeten worden aan de hand van een logische aanpak waarbij tevens gemeten kan worden of deze nog op koers ligt.
Risico	Zonder doelen en strategie zal de beoogde toekomstige situatie (de visie) waarschijnlijk niet gerealiseerd worden.

Parameter 3: Beleid

Het gegevensbeschermingsbeleid geeft aan op welke wijze voldaan wordt aan de van toepassing zijnde wet- en regelgeving. Input voor het gegevensbeschermingsbeleid zijn ook de doelen die de gemeente zichzelf gesteld heeft. Omdat de wet- en regelgeving externe factoren zijn die kunnen veranderen, is periodieke review nodig om vast te stellen of het beleid nog voldoet. Ook interne factoren, zoals onvoldoende effectiviteit van het beleid en gewijzigde visie, kunnen het nodig maken om te komen tot aanpassing van het beleid.

Concreet	De gemeente heeft beleid en procedures ontwikkeld en vastgesteld waarin is vastgelegd op welke wijze persoonsgegevens worden verwerkt en invulling wordt gegeven aan de wettelijke beginselen.
Doel	Het beleid dient ervoor om duidelijkheid te verschaffen over de inrichtingskeuzes van de bescherming van persoonsgegevens en te waarborgen dat de verwerking van persoonsgegevens op een rechtmatige wijze plaatsvindt.
Risico	Het ontbreken van een gegevensbeschermingsbeleid leidt ertoe dat er in de gemeente onduidelijkheid bestaat over wat precies wordt verwacht, waardoor de kans bestaat dat persoonsgegevens onrechtmatig worden verwerkt.

Parameter 4: Governance

Het waarborgen van de bescherming van persoonsgegevens ligt niet bij één persoon of de privacy-officers. Meerdere personen binnen de gemeente zijn in meer of mindere mate betrokken om aan de vereisten van de wet- en regelgeving te kunnen voldoen.

Concreet	De verdeling van de taken en verantwoordelijkheden en de rapportagelijnen zijn door de gemeente vastgelegd en vastgesteld.
Doel	Het doel van een heldere verdeling van taken en bevoegdheden en duidelijke rapportagelijnen is waarborgen dat op de juiste wijze invulling

	wordt gegeven aan de eisen van het gegevensbeschermingsbeleid en de AVG.
Risico	Door het ontbreken van een goede en inzichtelijke taakverdeling en rapportagelijnen is niet altijd duidelijk wie wat moet doen, waardoor de eisen van de AVG en het beleid niet effectief worden ingevuld.

Parameter 5: Mensen en middelen

De bescherming van persoonsgegevens legt beslag op de tijd van de medewerkers en middelen van de gemeente. Dit kan zijn door de extra inzet van medewerkers, het inschakelen van externe expertise of de aanschaf van bepaalde applicaties of systemen. Op basis van de governance-afspraken worden keuzes gemaakt in het toewijzen van de beschikbare schaarse middelen om de gewenste resultaten te behalen.

Concreet	Financiële middelen en medewerkers worden vrijgemaakt die de gemeente instaat stellen de werkzaamheden voor de bescherming van persoonsgegevens uit te voeren.
Doel	Voldoende in staat zijn om door middel van mensen en middelen uitvoering te kunnen geven aan het gegevensbeschermingsbeleid.
Risico	Geen of onvoldoende uitvoering kunnen geven aan het gegevensbeschermingsbeleid waardoor de voorgenomen doelen niet behaald kunnen worden.

Parameter 6: Risicomanagement

Het managen van risico's is een continu proces dat de risico's op het gebied van gegevensbescherming inventariseert, beoordeelt en een passende aanpak daarvan bewaakt. Risicomanagement richt zich op het beheersen van risico's bij het verwerken, waaronder verzamelen, opslaan en doorgeven van persoonsgegevens. Door middel van het toepassen van *Privacy by design* en het uitvoeren van DPIA's worden bij de ontwikkeling, de inrichting en de inzet van verwerkingen van persoonsgegevens de risico's in kaart gebracht en zoveel mogelijk beperkt dan wel weggenomen.

Concreet	De verwerkingsverantwoordelijke draagt zorg voor het beoordelen van de risico's op het gebied van gegevensbescherming, het treffen van passende maatregelen en het kunnen aantonen van het passend zijn van deze maatregelen. Privacy by design en DPIA's.
Doel	Beoordeling van de risico's (de kans x effect) is nodig om te bepalen hoe deze, door het treffen van maatregelen, teruggebracht kunnen worden tot binnen grenzen die de gemeente acceptabel acht.
Risico	Risico's worden niet of niet tijdig gesignaleerd, waardoor de verwerking van de persoonsgegevens niet aan de AVG voldoet en datalekken kunnen ontstaan; dit kan leiden tot gevaar voor de rechten en vrijheden van natuurlijke personen van wie de persoonsgegevens onrechtmatig worden verwerkt.

Parameter 7: Doelbinding

Het uitgangspunt van doelbinding is, dat gegevens worden verwerkt en verzameld voor een welbepaald, uitdrukkelijk omschreven en gerechtvaardigde doel. 'Welbepaald en uitdrukkelijk omschreven' houdt in dat men geen gegevens mag verzamelen zonder een precieze doelomschrijving. Het doel moet zijn bepaald alvorens men tot verzamelen overgaat. 'Welbepaald' houdt in dat deze doelomschrijving duidelijk moet zijn en niet zo vaag of ruim dat zij tijdens het verzamelproces geen kader kan bieden waaraan getoetst kan worden of de gegevens wel of niet nodig zijn voor dat doel. Het doel mag ook niet in de loop van het verzamelproces geformuleerd worden. 'Uitdrukkelijk omschreven' houdt in dat de gemeente het doel waarvoor de verwerking plaatsvindt, helder en duidelijk moet hebben omschreven.

Concreet	De verwerkingsverantwoordelijke heeft van alle verzamelingen en verwerkingen van persoonsgegevens tijdig, welbepaald en uitdrukkelijk omschreven doelen welke niet op verder op een met die doelen onverenigbare wijze mogen worden verwerkt.
Doel	Het telkens vaststellen van doelbinding is om te waarborgen dat persoonsgegevens alleen worden verzameld en (verder) verwerkt voor gerechtvaardigde doeleinden.
Risico	Het ongeoorloofd en onrechtmatig verzamelen en/of verder verwerken van persoonsgegevens.

Parameter 8: Register van verwerkingsactiviteiten

Om de naleving van de AVG aan te kunnen tonen dient de gemeente een register bij te houden van verwerkingsactiviteiten die onder haar verantwoordelijkheid plaatsvinden. Deze vastlegging maakt duidelijk hoe de verschillende organisatieonderdelen de werkprocessen ondersteunen en welke beveiligingsmaatregelen (op hoofdlijnen) zijn getroffen voor de verwerkingen en betrokkenen. Het register maakt tevens toezicht op de verwerkingsactiviteiten mogelijk.

Concreet	De gemeente heeft alle vereiste gegevens over de gegevensverwerkingen in een register vastgelegd. Dit register biedt een actueel en samenhangend beeld van alle gegevensverwerkingen, processen en technische systemen die betrokken zijn bij het verzamelen, verwerken en doorgeven van persoonsgegevens.
Doel	Het register van verwerkingsactiviteiten dient inzicht te verstrekken in de verwerkingen en de gegevensstromen binnen de gemeente en bij de partijen die namens de gemeente zorgen voor de verwerking van persoonsgegevens. Daarnaast dient het register een werkbaar instrument te zijn voor procesverantwoordelijken, privacyofficers en de functionaris gegevensbescherming. Ook biedt een compleet register een belangrijke

	waarborg voor het inwilligen van de rechten van betrokkenen.
Risico	Het niet hebben van een overzicht van verwerkingen leidt tot een incompleet beeld van de verwerkte categorieën persoonsgegevens en getroffen maatregelen voor de relevante verwerkingen, processen en technische systemen. Tevens komt hierdoor het inwilligen van de rechten van betrokkenen in gevaar.

Parameter 9: Kwaliteitsmanagement

Kwaliteitsmanagement zorgt voor de processen die bij onjuistheid en onnauwkeurigheid van de gegevens of bij ongewenste verwerking die gegevens rectificeren, volledig maken, wissen, de verwerking beperken of toestemming tot verwerking intrekken.

Concreet	De verwerkingsverantwoordelijke heeft kwaliteitsmanagement ingericht ten behoeve van de bewaking van de juistheid en nauwkeurigheid van persoonsgegevens. De verwerking is zo ingericht dat de persoonsgegevens kunnen worden gecorrigeerd, gestaakt, beperkt of overgedragen. Indien dit gebeurt op verzoek van betrokkene dan wordt deze over de status van de afhandeling geïnformeerd.
Doel	Kwaliteitsmanagement moet ervoor zorgen dat een gegevensverwerking correct en in overeenstemming met wettelijke bepalingen en de wens van betrokkenen is.
Risico	Wanneer persoonsgegevens onjuist of onnauwkeurig zijn ingevoerd of gecorrumpeerd raken, worden verkeerde conclusies over de betrokkene getrokken met nadelige gevolgen of naar het oordeel van betrokkene ongewenste verwerking van persoonsgegevens tot gevolg.

Parameter 10: Beveiliging

Informatiebeveiliging is het geheel van maatregelen, richtlijnen en procedures voor informatie en informatiesystemen, gericht op het waarborgen van de continuïteit van deze systemen en het voorkomen dan wel het beperken van de gevolgen van beveiligingsincidenten tot een acceptabel, vooraf bepaald niveau. Informatiebeveiliging spitst zich toe op de kernbegrippen beschikbaarheid, vertrouwelijkheid en integriteit.

Concreet	De verwerkingsverantwoordelijke treft technische en organisatorische maatregelen voor de verwerking van persoonsgegevens op een passend beveiligingsniveau.
Doel	Het beveiligen van de verwerking van persoonsgegevens is bedoeld om persoonsgegevens te beschermen tegen onbevoegde of onopzettelijke openbaring van, toegang tot, vernietiging van, verlies van toegang tot en wijziging van persoonsgegevens en enige andere vorm van onrechtmatige of onnodige verzameling en (verdere) verwerking.
Risico	Inbreuk in verband met persoonsgegevens (datalek): het ongewenst openbaar worden, manipulatie, misbruik, verlies en niet beschikbaar zijn

	van persoonsgegevens.

Parameter 11: Informatieverstrekking

Burgers en andere betrokkenen die persoonsgegevens verstrekken aan de gemeente hebben het recht te weten waarvoor, op welke wijze en door wie deze gegevens worden gebruikt. De gemeente heeft hiertoe een informatieplicht. Deze informatieplicht geldt ook wanneer persoonsgegevens van anderen worden ontvangen.

Concreet	De gemeente stelt voorafgaand aan elke verkrijging of verzameling van persoonsgegevens tijdig en op een vastgelegde en vastgestelde wijze informatie aan de betrokkene beschikbaar, zodat de betrokkene, tenzij een uitzondering geldt, toestemming kan geven voor de verwerking.
Doel	Informatie over de verkrijging en verzameling van persoonsgegevens wordt aan betrokkenen verstrekt om transparantie aan betrokkene te garanderen over de gegevensverzameling en de verwerking, zodat de betrokkene zijn rechten kan uitoefenen overeenkomstig de beginselen van behoorlijke en transparante verwerking.
Risico	Door te verzuimen transparantie te bieden, kan de gemeente niet verantwoorden en aantonen dat de gegevensverwerking voldoet aan de beginselen van behoorlijke en transparante verwerking.

Parameter 12: Bewaartermijnen

Persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk is om het doel te bereiken waarvoor ze zijn verzameld of niet langer dan de bewaartermijn die sectorspecifieke wetgeving stelt. De bewaartermijn kan worden beëindigd door actieve verwijdering van de gegevens of door het anonimiseren van de persoonsgegevens. Bij anonimiseren zijn de gegevens niet meer herleidbaar tot de betrokkenen.

Concreet	De gemeente hanteert ten aanzien van de verwerkingen van persoonsgegevens bewaartermijnen en treft de nodige maatregelen zodat deze niet worden overschreden.
Doel	Het hanteren en handhaven van bewaartermijnen borgt dat persoonsgegevens niet langer worden bewaard dan noodzakelijk is voor het te bereiken doel.
Risico	Onnodig bewaarde persoonsgegevens kunnen worden verwerkt voor andere dan de oorspronkelijke doelen.

Parameter 13: Doorgifte

Doorgifte kan plaatsvinden aan verwerkers en aan andere verwerkingsverantwoordelijken dan de gemeente. Een verwerker verricht de verwerking namens of in opdracht van een verwerkingsverantwoordelijke. In situaties waarbij meerdere verwerkingsverantwoordelijken

gezamenlijk de doelen en middelen voor de verwerking bepalen, zijn zij gezamenlijk verwerkingsverantwoordelijk.

Concreet	Bij doorgifte aan een andere verwerkingsverantwoordelijke zijn de onderlinge verantwoordelijkheden duidelijk en bij de doorgifte aan een verwerker zijn afdoende garanties geboden. Hiervoor worden data-leveringsovereenkomsten, onderlinge regelingen of verwerkersovereenkomsten getroffen.
Doel	De vereisten aan de doorgifte van persoonsgegevens waarborgen dat persoonsgegevens op een rechtmatige manier worden doorgegeven, op een juiste manier worden gebruikt en dat de verantwoordelijkheid voor deze rechtmatigheid en juistheid correct wordt neergelegd.
Risico	Het niet voldoen aan de vereisten leidt tot onduidelijkheid over de verantwoordelijkheden bij het doorgeven van persoonsgegevens waardoor de kans bestaat dat persoonsgegevens onrechtmatig worden doorgegeven en onrechtmatig verder worden verwerkt.

Parameter 14: Intern toezicht

Binnen de gemeente wordt toezicht gehouden op de rechtmatigheid van de gegevensverwerking. Een gegevensverwerking is rechtmatig als deze voldoet aan de eisen die door de AVG of sectorspecifieke wetgeving worden gesteld.

Concreet	De gemeente heeft een functionaris gegevensbescherming aangesteld. Deze functionaris ziet toe op de juiste naleving van de AVG en het gegevensbeschermingsbeleid. De functionaris gegevensbescherming hanteert een op risico gebaseerde aanpak en rapporteert periodiek over de stand van zaken met betrekking tot de naleving van de verordening.
Doel	Intern toezicht heeft als doel te controleren of er sprake is van rechtmatige, behoorlijke en transparantie verwerking van persoonsgegevens, en het aantoonbaar maken van naleving van het gegevensbeschermingsbeleid van de gemeente.
Risico	Als een verwerking van persoonsgegevens niet voldoet aan de eisen van de AVG, zijn de risico's tweeledig: enerzijds bestaat er gevaar voor de rechten en vrijheden van betrokkenen, anderzijds wordt de verwerkingsverantwoordelijke geconfronteerd met politiek-bestuurlijke en/of juridische gevolgen, verlies van vertrouwen en beschadiging van het imago.

Parameter 15: Rechten betrokkenen

Iedere betrokkene heeft (binnen grenzen van redelijkheid) het recht te weten of, door wie, waarvoor en op welke wijze zijn persoonsgegevens worden verwerkt. De verwerkingsverantwoordelijke moet hier transparant over zijn. Deze transparantie is nodig om de betrokkene of diens wettelijke vertegenwoordiger in staat te stellen zonder

onevenredige kosten en/of moeite zijn gegevens te laten corrigeren of de gemeente aan te spreken op de onrechtmatige verwerking van persoonsgegevens. Voorafgaand aan de verwerking van de persoonsgegevens worden betrokkenen geïnformeerd over de verwerking.

Concreet	De gemeente biedt de betrokkene informatie over de verwerking van persoonsgegevens en doet dit tijdig en in een passende vorm, zodat de betrokkene zijn rechten kan uitoefenen, tenzij er een specifieke uitzonderingsgrond geldt.
Doel	Transparantie over de verwerking van persoonsgegevens is noodzakelijk voor het kunnen uitoefenen van de rechten van betrokkenen.
Risico	Bij het ontbreken van transparantie over de verwerking van persoonsgegevens hebben betrokkenen geen inzicht in de rechtmatigheid van de verwerkingen, waardoor het vertrouwen in de dienstlening van de gemeente in het geding is.

Parameter 16: Datalekken

Het adequaat reageren op een datalek kan mogelijk nadelige gevolgen voor de betrokkenen voorkomen dan wel beperken. Een datalek is een "inbreuk in verband met persoonsgegevens": een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens. Datalekken moeten altijd gemeld worden. Hier geldt een drietrapsraket: altijd naar de privacy-officer en in bepaalde gevallen naar de Autoriteit Persoonsgegevens en/of de betrokkene(n).

Concreet	Bij een risico voor de rechten en vrijheden van de berokkenen meldt de verwerkingsverantwoordelijke een datalek binnen de daaraan gestelde termijn aan de Autoriteit Persoonsgegevens, documenteert de inbreuk, en informeert tevens bij een hoog risico de betrokkene. Vervolgens worden de juiste maatregelen genomen zodat dergelijke datalekken in het vervolg niet meer voorkomen.
Doel	Het doel van datalekken melden en registreren is nadelige gevolgen van een datalek te beperken dan wel te voorkomen. Door een adequate opvolging kunnen deze datalekken in de toekomst voorkomen worden.
Risico	Nadelige gevolgen voor de rechten vrijheden van betrokkene. Kans op herhaling binnen de gemeente.

Parameter 17: Bewustzijn

Een niet te onderschatten fundament voor het op de juiste wijze naleven van de AVG is draagvlak bij de medewerkers. Het is niet altijd vanzelfsprekend dat medewerkers begrip van en voor de bescherming van persoonsgegevens hebben. Daarom is het van groot belang dat medewerkers niet alleen door middel van allerlei vormen van voorlichting en educatie de

basisprincipes van de AVG leren kennen, maar ook dat hiermee begrip en draagvlak voor de bescherming van persoonsgegevens gecreëerd wordt.

Concreet	Het op regelmatige basis organiseren van voorlichtingsbijeenkomsten, interne opleidingen en activiteiten op het gebied van gegevensbescherming voor medewerkers die persoonsgegevens verwerken.
Doel	Het creëren van draagvlak voor en kennis van de bescherming van persoonsgegevens zodat de algemene beginselen van gegevensbescherming geïncorporeerd worden in de werkprocessen.
Risico	Geen draagvlak en kennis bij medewerkers waardoor geen uitvoering gegeven wordt aan de algemene beginselen van de AVG en verplichtingen zoals *privacy by design* met als gevolg datalekken.