# STAPPENPLAN VOOR GEMEENTEN BIJ DE VOORBEREIDING OP DE AVG

Versie 1.00 – 1 december 2017

Deze handreiking is mede tot stand gekomen door een samenwerking van onder andere VNG, KING, IBD en Kenniscentrum Europa Decentraal.

Voor meer informatie en vragen verwijzen we u naar de websites www.vng.nl en www.kinggemeenten.nl waar we u op de hoogte houden van alle nieuwe privacy ontwikkelingen. Indien u naar aanleiding van dit document vragen heeft, of advies wilt over de Wbp, AVG of privacy in het algemeen dan kunt u uw vragen stellen via het e-mailadres: privacy@kinggemeenten.nl

# STAPPENPLAN VOOR GEMEENTEN BIJ DE VOORBEREIDING OP DE AVG

Vanaf 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. Dit brengt voor gemeenten meer verplichtingen met zich mee bij het werken met persoonsgegevens. Dat vraagt een gedegen voorbereiding, waarbij het kan helpen om prioriteiten te stellen voor de te nemen maatregelen. Het doel van deze handreiking is om gemeenten hier een handvat voor te bieden in de vorm van een stappenplan. Gemeenten kunnen dit stappenplan gebruiken als hulpmiddel bij het maken van keuzes: wat moet eerst en wat kan later? Daarnaast biedt het een globaal overzicht van de belangrijkste maatregelen die gemeenten moeten nemen ter voorbereiding op de AVG. Het geeft ook aan waar in de voorbereiding de verschillende producten van KING van pas kunnen komen.

Het geadviseerde stappenplan voor gemeenten ziet er als volgt uit:


1. **Stel een Functionaris Gegevensbescherming (FG) aan**
2. **Stel een privacybeleid op en draag het uit**
3. **Stel een register van verwerkingen op (en hou het bij)**
4. **Pas de werkprocessen aan**
5. **Maak afspraken met derden**

In dit documenten worden de stappen uit dit plan verder toegelicht.

# 1 Stel een Functionaris Gegevensbescherming (FG) aan

Het aanstellen van een FG is onder de AVG, en dus per 25 mei 2018, verplicht. Het advies aan gemeenten is dan ook zo vroeg mogelijk een FG aan te stellen. Het aanstellen van de FG is in dit stappenplan niet alleen de eerste stap omdat het een wettelijke verplichting is, maar ook omdat de FG als interne toezichthouder op de verwerking van persoonsgegevens een drijvende rol speelt in alle volgende stappen. De FG heeft daarnaast een informerende en adviserende taak (AVG artikel 39), en kan fungeren als een centraal aanspreekpunt in het voorbereidingsproces.

Vaak is het bij het aanstellen van een FG de vraag of er al voldoende bewustwording is – zowel ambtelijk als bestuurlijk – op het gebied van privacy in het algemeen en de AVG in het bijzonder. Als dit niet zo is kan het wenselijk zijn om eerst een kwartiermaker/projectleider Implementatie AVG aan te stellen om tijdens de te nemen maatregelen ook aandacht te besteden aan het creëren van meer bewustwording. Daarbij is het belangrijk dat bestuurders weten wat de AVG betekent voor de organisatie, en wat mogelijke gevolgen zijn als er niet aan de wet voldaan wordt. Bij voldoende bewustwording zullen er eerder middelen vrij gemaakt worden om direct een FG aan te stellen. Over de precieze rol en taken van de FG, evenals de positionering van de FG in de organisatie is meer informatie beschikbaar in de specifieke handreiking hierover, te downloaden via de privacywebsite van KING.

Als er een FG is aangesteld dient deze ook aangemeld te worden bij de Autoriteit Persoonsgegevens (AP). De AP houdt een FG-register bij waarin alle aangemelde FG's per organisatie terug te vinden zijn. Hiermee is het aanstellen van een FG ook de makkelijkst controleerbare wettelijke verplichting uit de AVG. Als een gemeente over een FG beschikt zal de AP dat terecht als een signaal zien dat privacy serieus genomen wordt in de organisatie.

# 2 Stel een privacybeleid op en draag het uit

Transparantie en verantwoording zijn belangrijke uitgangspunten van de AVG. Gemeenten leggen verantwoording af over het gebruik van persoonsgegevens, onder andere door duidelijk te maken voor betrokkenen wat er met zijn of haar persoonsgegevens gebeurt. Door een privacybeleid en -reglement te publiceren maakt de gemeente duidelijk op welke manier zij met persoonsgegevens omgaat, en welke uitgangspunten daarbij gelden.

Daarnaast is een privacybeleid en -reglement opstellen meer dan transparant zijn naar, en verantwoording afleggen aan, burgers en ketenpartners. Het vervult ook binnen de organisatie een belangrijke rol: het beleid moet worden vastgesteld en is voor de FG hèt moment om (meer) bestuurlijke aandacht voor het onderwerp privacy te krijgen. Privacy is een onderwerp dat van belang is voor alle medewerkers van een gemeente door de gehele gemeentelijke organisatie en niet alleen van de FG of privacy officer. Dit houdt bijvoorbeeld in dat: het college van B&W eindverantwoordelijk is, de gemeenteraad zijn controlerende taken kan uitoefenen, de lijnmanagers gedelegeerd verantwoordelijk zijn, en er duidelijke privacyinstructies worden gegevens aan de professionals op de werkvloer. Zo komt privacy in de hele organisatie op de kaart. De FG speelt in dit proces een adviserende en toezichthoudende rol.

De privacyverklaring heeft betrekking op de gemeentelijke website(s). Wanneer de gemeente via de website privacygevoelige (persoons)gegevens verzamelt en/of opslaat, bijvoorbeeld via een online contactformulier, is een privacyverklaring wettelijk verplicht. Vanuit de privacywetgeving geldt namelijk de verplichting om klanten en bezoekers van de website duidelijk te informeren welke privacygevoelige gegevens verzameld worden en met welk doel dit gebeurt. Ook in situaties waarin een privacyverklaring niet verplicht is kan het toch lonen om er één te publiceren. In een dergelijk geval kunt u in de privacyverklaring aangeven dat er geen persoonsgegevens worden verwerkt.

Wanneer burgers op zoek zijn naar informatie over hoe de gemeente met 'privacy' omgaat zullen zij vaak als eerste kijken naar de privacyverklaring (zie ook de handreiking op de website van KING) op de website. Deze pagina is daardoor altijd goed te gebruiken als centrale plek om meer informatie over privacy te verstrekken. Denk hierbij bijvoorbeeld aan het publiceren van het beleid, reglement of een (publieke) versie van het register van verwerkingen. Op deze manier kan iedereen op één plek beter inzicht krijgen in de manier waarop de gemeente omgaat met persoonsgegevens.

KING heeft een model privacybeleid en -reglement gepubliceerd dat als basis kan worden gebruikt om het privacybeleid en de regels die daarvoor gelden te verduidelijken aan burgers en ketenpartners. Het document kan vervolgens op de website van de gemeente geplaatst worden voor iedereen die graag meer wil weten over hoe de gemeente omgaat met persoonsgegevens en privacy.

# 3 Stel een register van verwerkingen op (en hou het bij)

Het register is de centrale administratie waarin alle verwerkingen van persoonsgegevens binnen een gemeente in kaart zijn gebracht. Dit geeft overzicht en structuur. Hoewel het beheer van het register bij de FG is belegd, gebeurt het invullen ervan – vaak - in samenwerking met de verantwoordelijken voor de verwerkingen op de werkvloer. Het is belangrijk om het gesprek met de verantwoordelijken voor de verwerkingen aan te gaan, omdat op die manier gemeente-specifieke informatie aan het register kan worden toegevoegd. Het register is daarmee ook weer een perfecte gelegenheid om meer bewustwording omtrent privacy te creëren, en de bestaande verwerkingen nog eens goed te bekijken.

Het bijhouden van het register van verwerkingen is onderdeel van de verantwoordingsplicht van de gemeente. Het register kan ook nodig zijn als betrokkenen hun rechten uitoefenen. Eén van de maatregelen om invulling te geven aan de vereisten om betrokkenen actief te informeren zodra u persoonsgegevens gaat verwerken is het publiceren van een vereenvoudigde versie van het register op uw website. Op die manier geeft u ook uw burgers inzicht in welke persoonsgegevens de gemeente verwerkt. In de handreiking privacyverklaring is daarom al een verwijzing naar het register opgenomen.

Via de IBD-community kunnen gemeenten een deels ingevulde EXCEL-versie van het voorbeeldregister vinden. Gemeenten kunnen deze deels ingevulde versie ook opvragen via privacy@kinggemeenten.nl. Via de website van KING is er ook een handreiking met uitgebreide informatie over het register van verwerkingen en een uitleg bij de structuur van het voorbeeldregister beschikbaar.

# 4 Pas de werkprocessen aan

Alle verwerkingen zijn onderdeel van een proces, en die processen hebben eigenaren in de organisatie. Deze eigenaren (vaak lijnmanagers) zijn verantwoordelijk voor het borgen van privacy van de gegevens in deze processen. De FG functioneert ook hierbij als interne toezichthouder, en kan daarnaast adviseren en informeren. Als het register is ingevuld is er bekend welke verwerkingen in welke processen voorkomen. Deze processen moeten vervolgens worden nagelopen om te kijken hoe het best rekening kan worden gehouden met privacy en of wordt voldaan aan de eisen van de AVG. Er zullen veel processen moeten worden nagelopen, dus uiteraard is het verstandig om te beginnen bij de processen met het hoogste privacyrisico. De laatste versie van de Baselinetoets BIG biedt, onder het tabblad 'privacy', de mogelijkheid te beoordelen of een verwerking een verhoogd privacyrisico heeft. Het is de taak van de FG om toezicht te houden op het goed uitvoeren van dit proces.

Leg de bestaande procedures voor het borgen van privacy in werkprocessen – voor zover dit nog niet gebeurd is – vast, en zorg dat iedereen ze kent. Voorbeelden hiervan zijn bestaande procedures voor het doen van aanpassingen als een burger melding maakt dat zijn of haar gegevens niet kloppen (recht op rectificatie) of antwoord geven op de vraag of, en zo ja, welke gegevens van een burger zijn vastgelegd (recht op inzage), of overige processen gerelateerd aan de overige rechten van betrokkenen. Misschien staan deze procedures wel op papier, maar is de link met privacy nog niet gelegd. Verantwoording is een aandachtspunt binnen de AVG. Zorg dus dat u kunt aantonen dat er procedures zijn, dat iedereen ze kan vinden, en zich er ook aan houdt.

Er is niet één beste manier om werkprocessen met verwerkingen AVG-proof te maken. Wat wel of niet past én werkt is sterk afhankelijk van de context, en kan dus per gemeente verschillen. Er zijn vaak verschillende opties en overwegingen, waaruit een keuze gemaakt moet worden. Zodra in kaart is gebracht welke verwerkingsprocessen er zijn en is geanalyseerd waar zich de grootste privacyrisico's voordoen, betreffen deze keuzes bijvoorbeeld de maatregelen die nodig zijn om deze risico's tot een aanvaardbaar niveau te beperken, of welke alternatieve verwerking hetzelfde resultaat levert tegen een lager risico. Hierbij is het aan te raden om het 'pas-toe-leg-uit principe' te hanteren: leg goed vast waarom een bepaalde keuze omtrent privacyaspecten gemaakt wordt. Betrek in ieder geval de juiste mensen bij het maken van deze keuzes: denk aan de FG, de CISO, CIO, ICT-adviseurs, lijnmanagers en juristen. Goed nadenken over privacy, hier de discussie over aangaan, en vervolgens een weloverwogen keuze maken is naast alle verplichtingen een belangrijke bedoeling van de AVG.

Tot slot is het met het oog op de toekomst een goed idee om direct een terugkerend moment in te bouwen in de planning en control-cyclus voor de evaluatie van alle privacy-maatregelen. Eventueel kunt u hiervoor zelfs een aparte cyclus inrichten, bijvoorbeeld volgens het Plan-Do-Check-Act model. Dit zorgt ervoor dat de organisatie blijft voldoen aan de AVG, gemakkelijk kan inspelen op veranderingen op het gebied van privacy in omgeving en organisatie, en dat al het werk dat nu in

de voorbereiding gaat zitten niet over een aantal jaar volledig opnieuw gedaan moet worden. Uiteraard is de FG altijd actief als toezichthouder op dit gebied, maar alleen door ook structureel organisatiebreed privacy op de agenda te houden wordt privacy echt verankerd in de organisatie.

# 5 Maak afspraken met derden

In deze stap gaat het allereerst om het bepalen wanneer een verwerkersovereenkomst nodig is. Daarvoor moet worden vastgesteld of de betreffende derde een verwerker of verwerkingsverantwoordelijke is. De regel is dat de verwerkingsverantwoordelijke het doel en de middelen voor de verwerking vaststelt. Een verwerkersovereenkomst is alleen nodig als de derde partij verwerker is. Is de derde partij zelf verwerkingsverantwoordelijke dan is een verwerkersovereenkomst niet nodig, maar wordt wel aanbevolen om op een andere wijze afspraken te maken over de zorgvuldige omgang met persoonsgegevens. Dit kan bijvoorbeeld in de standaard inkoopvoorwaarden. In de Gemeentelijke Inkoopvoorwaarden bij IT (GIBIT) zijn al enkele specifieke artikelen opgenomen over privacy, beveiliging en archivering.

Om te weten voor welke verwerkingen verwerkingsovereenkomsten nodig zijn, kan het register van verwerkingen worden geraadpleegd. Dit geeft bovendien inzicht in waar verwerkersovereenkomsten voor nodig zijn, welke bijna aflopen, en voor welke verwerkingen al afspraken zijn gemaakt. Gebruik het register om systematisch inzicht te krijgen in alle verwerkersovereenkomsten die opgesteld zijn binnen de gemeenten, en om het gesprek aan te gaan bij nieuwe verwerkersovereenkomsten. Wederom geldt bij deze stap: betrek de juiste mensen bij het proces! Denk hierbij bijvoorbeeld aan de afdeling inkoop/ leveranciersmanagement, en de juridische afdeling, privacy officer of CISO.

De IBD heeft een model verwerkersovereenkomst opgesteld dat gemeenten een handvat biedt en een uitgangspunt om de eigen specifieke verwerkersovereenkomst vorm te geven. Deze verwerkersovereenkomst is gebaseerd op het gemeenschappelijke normenkader voor informatiebeveiliging, de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). De laatste versie van deze toets (v1.3) is in lijn gebracht met de AVG. De IBD heeft daarnaast een factsheet uitgebracht over verwerkersovereenkomsten. Deze factsheet geeft antwoord op de vraag wanneer er wel en wanneer er geen verwerkersovereenkomst noodzakelijk is. Het document bevat een groot aantal voorbeelden van situaties die in de gemeente kunnen voorkomen. Op de website van de IBD komt ook het verschil tussen verwerker en verwerkingsverantwoordelijke uitvoerig aan bod.

# Tot slot

Het is onvermijdelijk dat u in de praktijk tegen vragen of problemen aanloopt. Hierin bent u zeker niet de enige, dus het kan helpen om ervaringen uit te wisselen en kennis te delen. Wie weet heeft een collega-gemeente al een slimme oplossing gevonden voor een probleem waar u niet uitkomt. Door met elkaar te praten, discussiëren, en elkaar te helpen voorkomen we dat iedereen het wiel zelf uit moet vinden, en stimuleren we nadenken over privacy.

Uiteraard is kennis delen binnen het gemeentelijke netwerk niet alleen belangrijk in de aanloop naar 25 mei 2018, maar zal het ook na deze datum een belangrijke rol blijven spelen bij het verder werken aan privacy. Reden genoeg dus om hier serieus aandacht aan te besteden!

De IBD-community maakt het niet alleen mogelijk om documenten makkelijk te delen, maar ook om ideeën, kennis, adviezen en tips uit te wisselen, vragen te stellen en problemen waar u tegenaan loopt te bespreken. Denk hierbij aan vragen over het invullen van het register, maar ook bijvoorbeeld over het privacybeleid en reglement. Daarnaast zijn er discussies over actuele onderwerpen, zoals datalekken en het inzagerecht. Uiteraard kunt u ook zelf een discussie starten. Om elkaar makkelijker te kunnen deelnemers van de community aangeven welke rol ze binnen hun organisatie vervullen, dat kan ook voor de rol van Functionaris Gegevensbescherming - als u dat doet bent u als FG vindbaar voor andere deelnemers van de community.

KWALITEITS
INSTITUUT
NEDERLANDSE
GEMEENTEN

**VNG / KING**

**NASSAULAAN 12**
**2514 JS  DEN HAAG**

**POSTBUS 30435**
**2500 GK  DEN HAAG**

**T 070 373 80 08**

**PRIVACY@KINGGEMEENTEN.NL**
**WWW.KINGGEMEENTEN.NL**