Privacy notitie

'zorgvuldig en transparant'

Gemeente Renkum

april 2018

Inhoud

Voorwoord

Het beschermen van de privacy en de gegevens van onze inwoners waarover wij beschikken uit hoofde van de uitvoering van onze taken is gebonden aan strenge wet en regelgeving. Maar meer nog dan dat is het ingegeven vanuit een grondhouding van respect. Privacy en de daaraan gekoppelde gegevens zijn een weerspiegeling van onze inwoners als persoon en van hun persoonlijke levenssfeer.

Immers, sociale interacties zijn voor een groot deel gebaseerd op privacy. Iemands reputatie beïnvloedt de kansen, relaties en vriendschappen die hij/zij heeft. Van nature creëert men grenzen in omgang met anderen en hanteert men andere omgangsvormen en gebruiken afhankelijk van de omgeving waarin men zich bevindt. Er wordt dus een bewuste keuze gemaakt in wat wij persoonlijk delen of niet delen: privacy. Privacy helpt ons deze grenzen te hebben. Inbreuken op deze grenzen leiden tot ongemakkelijke sociale situaties en kunnen onderlinge relaties van inwoners beschadigen.

De vrijheid van elke inwoner om andere meningen of ideeën te onderzoeken of ervaren hangt voor een groot deel samen met privacy. Wanneer men ervaart dat alles in de gaten gehouden of beoordeeld wordt, is er druk om binnen de gevestigde paden te blijven. De mogelijkheid om kritiek te uiten, zonder dit noodzakelijkerwijs met de hele wereld te delen, is essentieel in de ontwikkeling van nieuwe denkwijzen en innovaties. Dit argument gaat ook op met betrekking tot politiek: één van de redenen waarom men in een afgesloten stemhok kan stemmen is omdat men zo volledig vrij is te stemmen op wie men wil en niet onderhevig is aan druk van de omgeving.

Zo hangt privacy ook samen met persoonlijke ontwikkeling: niet iedereen maakt op alle momenten in zijn leven de juiste keuzes. Het feit dat deze keuzes privé kunnen blijven staat ons toe deze keuzes bij te sturen of onze mening aan te passen. Privacy geeft ons de mogelijkheid tot ontwikkeling en groei zonder noodzakelijk geconfronteerd te worden met keuzes uit het verleden.

Kortom privacy staat ons als inwoner toe te controleren wie wanneer over welke informatie over ons kan beschikken. Dat past ook bij de eigen regie die wij als inwoner over ons leven willen hebben. Als gemeente zijn wij ondersteuner, dienstverlener en op onderdelen beschermer en moeten wij met privacy van onze inwoners zeer zorgvuldig omgaan.

De wetgeving inzake de bescherming van persoonsgegevens en privacy is helder voor wat betreft dat wat wij moeten regelen in processen en systemen. Blijft ons een keuze te maken wat voor soort gemeente wij willen zijn. Deze notitie geeft daarop antwoord in hoofdstuk 5. De overige hoofdstukken gaan in op de wetgeving en betekenis in zijn algemeenheid voor onze inwoners en onze organisatie. Daarmee wordt de context beschreven waarbinnen wij werken en handelen.

1 Inleiding

Vanaf 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG van 24 mei 2016) van toepassing en is de Uitvoeringswet gegevensbescherming van kracht. Dat betekent dat er vanaf die datum op basis van de AVG dezelfde privacywetgeving geldt in de hele Europese Unie (EU). De Wet bescherming persoonsgegevens (Wbp) geldt dan niet meer. Omdat wij veel persoonsgegevens verwerken moeten wij onze organisatie op de eisen van de AVG en de Uitvoeringswet inrichten. Dit betekent niet dat wij op dat moment 100% 'privacy proof' moeten zijn maar wel dat we de goede stappen hebben gemaakt in die richting en daar verder gestructureerd uitvoering aan geven.

Bescherming van persoonsgegevens is niet nieuw, maar in de AVG wordt een aantal zaken scherper geformuleerd zoals het recht van de inwoner om 'vergeten te worden', het recht om inzage in zijn persoonsgegevens te hebben, het recht om verwijderen of veranderen van zijn persoonsgegevens en transparantie en verantwoording van de zijde van de gemeente. Het goed en duurzaam inrichten en bijhouden van een register over alle verwerking van persoonsgegevens speelt hierbij een belangrijke rol. Maar ook onze contracten met externe partijen die voor ons persoonsgegevens verwerken moeten tegen het licht worden gehouden en indien nodig aangepast. Denk daarbij bijvoorbeeld aan IT-hosting en salarisgegevens.

Omdat zowel de Uitvoeringswet als de AVG de rechten en plichten zo goed als uitputtend beschrijven, is er weinig ruimte voor lokale beleidsruimte. Wel kan vanuit de wens hoe je als gemeente erin staat een richtlijn worden geformuleerd op basis waarvan de wetgeving binnen de organisatie wordt geïmplementeerd (zie ook conclusies en aanbevelingen van de RTA van juni 2016, bijlage 1).

Deze nota voorziet daarin. Vanuit een schets van het belang van de bescherming van privacy en de wettelijke kaders komen wij tot een richting voor inrichting, waarbij de bescherming van privacy, de openheid naar onze inwoners en het belang van het maatwerk binnen de afwegingen die steeds gemaakt moeten worden in goede balans zijn met elkaar. Hierbij is rekening gehouden met de conclusies en aanbevelingen van de RTA van juni 2016 zoals ook aangegeven in de raadsbrief van oktober 2017 (bijlage 2). Deze nota ziet daardoor voornamelijk op het menselijk handelen in het kader van de bescherming van privacy als een 'way of life' (privacy) naast aandacht voor informatiebeveiliging wat meer gericht is op systemen en (werk)processen.

De nota is als volgt opgebouwd. We zoomen in hoofdstuk 2 eerst in op de basis van de AVG, het belang van de bescherming van privacy. Dat belang heeft geleid tot een wetgevend kader dat in hoofdstuk 3 kort de revue passeert om een context te schetsen. In hoofdstuk 4 wordt het onderscheid tussen privacy en informatiebeveiliging nader toegelicht. Hoofdstuk 5 is de vertaling van de conclusies en aanbevelingen van de RTA en belicht de principes van privacy van waaruit wij als organisatie willen handelen. Hoofdstuk 6 richt zich op de implementatie gebaseerd op de bevindingen uit de Quick Scan en het onderzoek van BMC uitgewerkt wordt in plannen van aanpak en uitvoeringsplannen voor de verschillende domeinen. Als laatste geven wij in hoofdstuk 7 de vindplaatsen met een korte intro voor meer informatie.

2 Wat is privacy en waarom is bescherming belangrijk?

Privacy is een grondrecht. Artikel 10 van de Nederlandse Grondwet stelt dat ieder, behoudens bij of krachtens de wet te stellen beperkingen, recht heeft op eerbiediging van zijn persoonlijke levenssfeer. Ook al zeggen burgers vaak 'ik heb niets te verbergen', toch is het belangrijk om privacy van inwoners zeer serieus te nemen omdat daar nu eenmaal meer facetten aan kunnen zitten dan men oppervlakkig gezien denkt. Bescherming van privacy stelt iedere inwoner in staat om zelf te bepalen wie wanneer over welke informatie van hem kan beschikken, behoudens daar waar de wet uitdrukkelijk voorschrijft dat persoonlijke gegevens noodzakelijk zijn voor de uitvoering van specifiek die wet.

2.1 Grenzen aan gebruik gegevens

Persoonlijke informatie is een belangrijk onderdeel van informatie over inwoners en de keuzes die zij maken in het kader van een hulpvraag of aanvraag die zij bij ons doen. Het bijeenbrengen van informatie is echter wel gebonden aan het uitgangspunt dat die kennis alleen gebruikt mag worden voor het doel waarvoor het is verkregen en dat niet meer gegevens worden verzameld en vastgelegd dan absoluut noodzakelijk voor het behandelen van de aanvraag.

Geaggregeerde en geanonimiseerde informatie met betrekking tot (groepen) inwoners daarentegen is van belang voor het formuleren van beleidsrichtingen en het onderbouwen van keuzes of verantwoording (data analyse en –sturing) en mag wel gebruikt worden voor diverse doelen.

2.2 Conclusie

Privacy betreft de hele persoonlijke levenssfeer van onze inwoners en een schending daarvan kan verstrekkende gevolgen hebben voor hun persoonlijke ontwikkeling en sociaal maatschappelijke status. Niet voor niets is privacy een grondrecht. Daarom is het van belang dat wij ons daarvan bewust zijn, daarnaar handelen en dat onze IT zo is georganiseerd dat de bescherming van privacy optimaal is ingericht.

3 Wettelijk- en regelgevend kader

Privacy is een grondrecht en tot mei 2018 wettelijk ingekaderd via de Wet bescherming persoonsgegevens (Wbp). De Wbp is de Nederlandse implementatie van de Europese privacyrichtlijn uit 1995. Vanaf 25 mei 2018 is deze richtlijn vervangen door de Europese Verordening Gegevensbescherming (AVG). De Wbp geldt vanaf die datum niet meer.

3.1 Europese Algemene Verordening Gegevensbescherming (AVG)

Mei 2016 is de Europese Algemene Verordening Gegevensbescherming (AVG) vastgesteld. Deze is op 25 mei 2018 van toepassing geworden voor alle lidstaten. De AVG borduurt voort op de eerdere richtlijn en de Nederlandse Wet bescherming persoonsgegevens (Wbp). Feitelijk vormt de AVG een uitbreiding daarop. De verordening zorgt voor versterking van de privacyrechten van inwoners rondom toestemming en verwijdering van persoonsgegevens. Daarnaast regelt de verordening dat organisaties meer verantwoordelijkheden krijgen in het aantonen dat zij gegevensverwerking op orde hebben (documentatieplicht). Een groot aantal organisaties, zoals gemeenten, moet een functionaris gegevensbescherming (FG) aanwijzen.

3.2 Gegevensverwerking

Voor elke verwerking van persoonsgegevens is een wettelijke grondslag nodig. Daarnaast mogen gegevens alleen verwerkt worden als zij noodzakelijk zijn voor een bepaald, concreet omschreven doel (doelbinding), niet meer dan strikt nodig voor dat doel (proportionaliteit) en niet op een andere minder nadelige wijze kunnen worden verwerkt (subsidiariteit). Voor gegevensverwerking die domein overstijgend is bestaat formeel (nog) geen specifieke wettelijke grondslag. In deze situatie vallen wij terug op de algemene bepalingen uit de AVG: zorgvuldige belangenafweging, toetsen aan rechtmatigheid en doelmatigheid.

De gemeente is verplicht altijd transparant te zijn over de gegevens die zij van inwoners verwerkt. Inwoners hebben te allen tijde het recht inzage te hebben in hun gegevens, deze te wijzigen en / of te laten verwijderen tenzij de wet zich daartegen verzet of de gegevens simpelweg nodig zijn om hun aanvraag te kunnen behandelen.

3.3 Rol Functionaris Gegevensbescherming

De Functionaris gegevensbescherming (FG) ziet toe op verwerking van persoonsgegevens conform de wet met inbegrip van de finaliteit (bewaartermijn) en proportionaliteit van de verwerking van volledige en nauwkeurige gegevens. De FG fungeert als een waakhond van de gegevensverwerking. Daarvoor is bepaalde mate van onafhankelijkheid nodig ten opzichte van de afdelingen die de gegevens verwerken. In positionering van deze functionaris is dit een aandachtspunt. In Renkum zal BMC tot de datum van inwerkingtreding van de AVG optreden als kwartiermaker FG. In dat kader doet BMC een aanbeveling voor de positionering van de FG zodat wij aansluitend daarop een FG kunnen aanwijzen.

3.4 Maatwerk bescherming persoonsgegevens

De AVG biedt ruimte om afwegingen te maken. De verwerking en het gebruik van persoonsgegevens kan van casus tot casus verschillen. De afwegingen kunnen alleen door professionals op de werkvloer, die de context kennen, gemaakt worden. Deze context moet expliciet aanwezig zijn en vastgelegd. Hierover is geen algemeen beleid te ontwikkelen, hoogstens richtlijnen. Goede richtlijnen moeten ontstaan uit reflectie op de praktijk. Voorlopig gaat het om de argumentatie van elk apart geval. Jurisprudentie zal in de toekomst moeten uitwijzen waar grenzen liggen.

3.5 Conclusie voor uitvoering

Onder de AVG hebben onze inwoners diverse rechten waar zij beroep op kunnen doen zoals het recht op inzage, het recht op rectificatie, het recht op beperking van de verwerking, het recht op wissing van de gegevens (het recht om ‘vergeten te worden’), het recht op intrekken van toestemming en het recht op bezwaar. Hiertoe moeten wij een transparante procedure ontwikkelen.

Wij blijven onder de Verordening verantwoordelijk voor een goede beveiliging van persoonsgegevens. De juistheid van de gegevens moet geborgd zijn o.a. tegen ongeoorloofde of onrechtmatige verwerking (bijvoorbeeld tegen ‘indringers’ die gebruik willen maken van persoonsgegevens maar daartoe niet geautoriseerd zijn (waaronder hackers)) en tegen onopzettelijk verlies. Wij moeten hierover verantwoording kunnen afleggen en inbreuken op de beveiliging moeten, net als nu het geval is, gemeld worden bij de Autoriteit Persoonsgegevens en betrokkenen.

4 Informatiebeveiliging en privacy

Informatiebeveiliging is breder dan privacy. Het omvat alle informatie en niet alleen persoonsgegevens en is meer gericht op de technische kant. Fouten op het gebied van verwerking van persoonsgegevens kan schade berokkenen aan inwoners. En de meeste fouten worden veroorzaakt door (onzorgvuldigheid, onoplettendheid) van mensen.

4.1 Risico sturing

Bescherming van persoonsgegevens is een onderwerp dat breed en diep in onze gemeentelijke organisatie aandacht verdient. Het raakt sterk aan informatiebeveiliging en maakt er onderdeel van uit. Het is ondoenlijk voor alle situaties waar mogelijk fouten gemaakt kunnen worden op het gebied van verwerking van persoonsgegevens richtlijnen, protocollen en systeembeveiligingen in te voeren. In lijn met hoe informatiebeveiligingsbeleid geacht wordt te worden opgebouwd kiezen wij voor een risico-gestuurde aanpak. Dat betekent dat op basis van periodieke analyse de risico's in beeld worden gebracht. En dat juist op de grootste risico's maatregelen worden genomen om die risico's in te perken.

Deze aanpakt past goed bij de wijze waarop het wetgevend kader in de AVG is ingericht. Risico-gestuurd werken legt nadruk op mens, cultuur, flexibiliteit, leren, aanpassingsvermogen en de realiteit van begrensde maakbaarheid van organisaties. De AVG, evenals de Wbp voorheen, geeft ruimte voor afweging door de professionals. Richtlijnen voor afwegingen tussen hulpen zorg verlenen, ondersteuning bieden en gelijktijdig recht doen aan bescherming van persoonsgegevens zal in de praktijk van de komende jaren via ervaring en jurisprudentie inhoud krijgen. En tot slot is een risico-gestuurde aanpak in lijn met de Baseline Informatiebeveiliging (BIG), zoals die voor gemeenten geldt (https://informatiebeveiliging-gemeenten.nl/baseline-informatiebeveiliging).

4.2 Informatievoorziening en verantwoording

We bedden de risico-gestuurde aanpak in in ons kwaliteitsgericht werken en in onze planning & controlcyclus. Op deze manier borgen we dat privacy blijvend onder de aandacht blijft en dat nieuwe risico's tijdig in beeld komen en we er maatregelen op nemen. Dit gebeurt via periodiek evaluaties / audits. Door koppeling met de risicoparagraaf in de begroting en jaarrekening van de gemeente borgen we dat periodiek inzicht in de stand van zaken van de bescherming van persoonsgegevens.

4.3 Conclusie

Nadat het veld van gegevensbeheer volledig is doorgelicht en ingericht, implementeren we een op risico gebaseerde aanpak in toezicht en controle op de uitvoering vanuit het gezichtspunt van informatiebeveiliging. Op het gebied van privacy, het menselijk handelen, sturen wij op bewust handelen.

5 Principes van privacy

Om de veiligheid van privacy te waarborgen handelen wij vanuit de volgende principes:

5.1 Ontwikkelrichting: eigenaarschap van begrip en eigen verantwoordelijkheid

Wij willen ons ontwikkelen vanuit het eigenaarschap van begrip en eigen verantwoordelijkheid.
Van daaruit werken wij toe naar handelen vanuit onbewuste competentie, kennis is zo sterk ingebed in het handelen dat wij daarover niet meer krampachtig hoeven na te denken. Aandacht voor de bescherming van privacy is automatisme.

Wij werken vanuit eigenaarschap en verantwoordelijkheid waarop bewust wordt gestuurd en dat bewust wordt geborgd.

State of the art
Uit de Quick Scan is naar voren gekomen dat de fase van onbewust incompetent (niet weten dat je het niet weet) is gepasseerd, dat wij ons bevinden in een fase tussen bewust incompetent en bewust competent, waardoor er een positief kritisch lerende houding is.

5.2 Zorgvuldig en transparant

Wij zijn ons bewust van het belang van zorgvuldig en transparant omgaan met persoonlijke gegevens van en voor onze inwoners. Dat willen wij ook laten zien. Daarom maken wij dat kenbaar in al onze in onze communicatie.

Wij zijn open en duidelijk naar onze inwoners over hoe wij met hun gegevens omgaan, waar wij gegevens opslaan en met welk doel. Wij informeren onze inwoners over hun rechten en over de wijze waarop zij hun rechten kunnen uitoefenen.

State of the art
Uit de Quick Scan blijkt dat wij onvoldoende helder maken aan onze inwoners hoe wij dit doen. Ook is er onvoldoende informatie op onze gemeentelijke site ter informatie van onze inwoners aanwezig.

5.3 Bescherming veiligheid

Het is niet altijd eenvoudig om een goede balans te vinden tussen het waarborgen van de privacy van alle betrokkenen enerzijds, en het bieden van veiligheid aan onze inwoners anderzijds. Uitgangspunt in de AVG is data-minimalisatie: verwerk niet meer gegevens dan nodig is en deel deze gegevens met zo min mogelijk medewerkers. In situaties waarbij de veiligheid en/of gezondheid van inwoners worden bedreigd, kan het nodig zijn om informatie te delen. Daarbij dragen wij zorg voor een zorgvuldige dossiervorming en motivering.

Als er zorgen zijn rond de veiligheid van inwoners, met name als het gaat om kwetsbare groepen zoals bijvoorbeeld kinderen, weegt het belang van deze personen in de afweging zwaar mee.

State of the art
Uit de Quick Scan blijkt dat het omgaan met persoonsgegevens stress oplevert. De afweging wat wel en wat niet vastleggen speelt daarbij een rol. Daarbij kan diezelfde stress voorkomen bij het wel of niet

delen van informatie. Daarin is de wetgever feitelijk wel heel duidelijk, als de veiligheid van een persoon ongeacht de leeftijd in geding is en het delen van informatie draagt bij aan het geven of borgen van veiligheid, dan is dit mogelijk, op voorwaarde dat de gemeente de belangen van alle betrokkenen voldoende heeft afgewogen en op voorwaarde dat deze belangenafweging in het dossier wordt vastgelegd.

5.4 informatiebeveiliging

De Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) is leidend voor de aanpak informatiebeveiliging (zie ook hfdst 7).

De informatiebeveiliging wordt conform de eisen (BIG) die hiervoor gelden uitgevoerd en geborgd.

State of the art
Wij maken gebruik van beveiligde mail, beveiligd printen en van een register voor data opslag.
BMC voert het onderzoek naar informatie beveiliging uit en vervult tijdelijk ook de rol van FG. Zij leveren een rapportage op basis waarvan het uitvoeringsplan informatiebeveiliging wordt opgesteld.

6 Implementatie

De AVG schrijft een aantal zaken dwingend voor, zoals bijvoorbeeld:

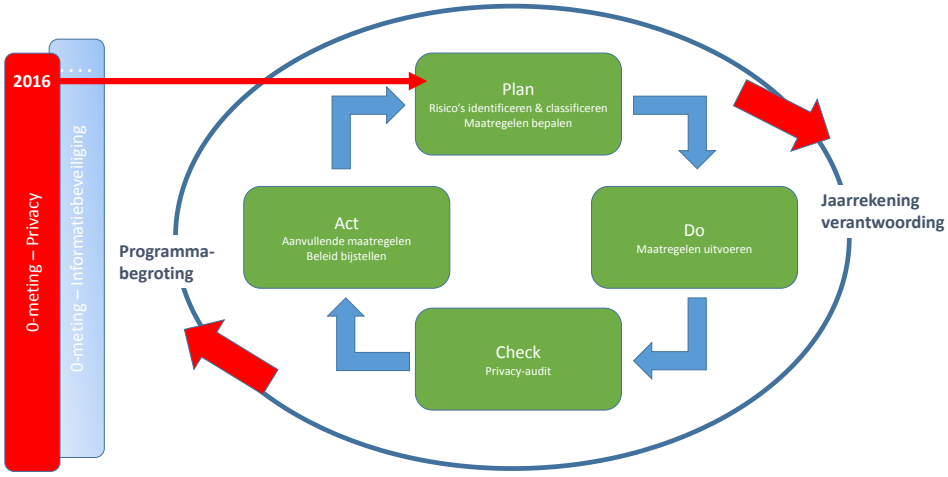
- een intern gegevensbeschermingsbeleid (proces) vast te stellen,
- een functionaris voor gegevensbescherming (afgekort als FG) aan te stellen;
- privacy te integreren als vast onderwerp binnen de bedrijfsvoering en de werking ervan jaarlijks te controleren;
- een gegevensbeschermingseffectbeoordeling(GEB) (voorheen privacy impact assessment afgekort als PIA) uit te voeren op het moment dat er veranderingen in diensten, producten, processen en informatiesystemen worden doorgevoerd (denk hierbij bijvoorbeeld aan het migreren van informatie naar de cloud, of het aanschaffen van een nieuw informatiesysteem).

De uitwerking hiervan en de uitwerking van deze richtlijn (hoofdstuk 5) is de taak van het college. Het college stuurt de uitvoering via een uitvoeringsplan. Het uitvoeringsplan is gebaseerd op een 0-meting privacy (Quickscan) die in de hele organisatie is uitgevoerd. De samenwerking met netwerk- en ketenpartners is in deze 0-meting betrokken. In de 0-meting is in onderlinge samenhang gekeken naar de processen, de medewerkers (hebben zij kennis van privacy-gevoeligheden en handelen zij hier bewust en zorgvuldig in) en naar de inrichting van de governance. In het kader van bewustwording (zie onder hfdst 5 1^{e} principe) is in het sociaal domein gestart met het ‘privacy spel’ dat door alle coördinatoren, coaches en consulenten wordt gedaan. Daarnaast is gestart met de bewustwordingscampagne ‘Safe and Sound’ waar alle werknemers aan deelnemen. Door de anonieme aggregatie het toets element hebben wij tevens een 2^{e} 0-meting waaraan dan alle medewerkers hebben deelgenomen.

Een eventueel later uit te voeren 0-meting op het gebied van informatiebeveiliging kan via dezelfde

aanpak worden gedaan en zo de basis vormen voor een inbedding in de verbeter-, sturings- en verantwoordingsscyclus.

In onderstaande figuur is het overzicht van de implementatie-aanpak weergegeven.



6.1 Uitvoering

Met als eerste de Quick Scan is een ex ante evaluatie over kennis en bewustzijn van privacy binnen onze organisatie gemaakt. Deze geeft van zaken met betrekking tot privacy waar het gaat om privacy aspecten in contracteren, bewust handelen en dossiervorming aan waar de organisatie staat.
Vanuit deze ex ante evaluatie is het mogelijk de vinger te leggen op plekken die aandacht nodig hebben en aan te wijzen waarop moet worden ingezet om te verbeteren. Deze zijn in het Plan van Aanpak voor sociaal domein nader uitgeschreven en met de stakeholders besproken en geprioriteerd. Daarbij is duidelijk geworden dat er tussen de punten bewustwording, processen en dossiervorming een sterke samenhang is. Aandacht voor privacy is daarbij een blijvend punt van aandacht dat bewaakt moet worden.

Aan BMC is opdracht gegeven tot het ondersteunen bij de implementatie van de AVG, met als resultaat het bereiken van een adequaat uitvoeringsniveau AVG. Aan de hand van hun bevindingen volgt een aantal plannen van aanpak voor de betrokken domeinen.

De vooruitgang die op basis van de plannen van aanpak wordt gemaakt wordt gevolgd en bijgestuurd vanuit de bewuste kritische houding van de teams zelf, vanuit de coördinatie en vanuit het management.

7 Voor nadere informatie

Dossier BIG

(https://informatiebeveiliging-gemeenten.nl/baseline-informatiebeveiliging)

In november 2013 is tijdens de Buitengewone Algemene Ledenvergadering (BALV) van de Vereniging van Nederlandse Gemeenten (VNG) de Resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' bekrachtigd. Deze Resolutie, die is opgesteld door de Vereniging van Nederlandse Gemeenten (VNG) in samenwerking met de Informatiebeveiligingsdienst voor gemeenten (IBD) en de Taskforce Bestuur en Informatieveiligheid Dienstverlening (Taskforce BID) houdt in dat iedere gemeente het informatiebeveiligingsbeleid vaststelt aan de hand van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG), die is opgesteld door de IBD. Tevens zullen gemeenten informatieveiligheid zowel bestuurlijk als ambtelijk borgen en maken ze de invulling op informatieveiligheid transparant voor burgers, bedrijven en ketenpartners.

VNG: Dossier Privacy/AVG

(https://vng.nl/onderwerpenindex/dienstverlening-en-informatiebeleid/privacy-avg) Themapagina van de VNG over de implementatie van de AVG bij gemeentelijke organisaties.

Autoriteit persoonsgegevens:

AP: Dossier AVG (https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving)

AP: Over Privacy (https://autoriteitpersoonsgegevens.nl/nl/over-privacy/persoonsgegevens)