Nieuwegein
GEMEENTEBLAD
Officiële uitgave van de gemeente Nieuwegein

Nr. 1674
4 januari
2019

Besluit van het college van bugemeester en wethouders van de gemeente Nieuwegein houdende regels omtrent omgaan met persoonsgegevens Beleidsplan veilig omgaan met persoonsgegevens in de gemeente Nieuwegein

1. Inleiding

In de afgelopen decennia hebben technische ontwikkelingen een hoge vlucht genomen. Het is steeds eenvoudiger geworden om informatie, waaronder informatie over personen, via ICT-middelen te delen met anderen, op te slaan in bestanden of te combineren met andere informatie die (vanuit openbare bronnen) beschikbaar is.
In de Wet bescherming persoonsgegevens van 6 juli 2000 (welke is afgeleid van de Europese databeschermingsrichtlijn uit 1995) is een eerste poging ondernomen om op nationaal niveau grip te krijgen op het verwerken van persoonsgegevens. Deze wet stamt uit een tijd dat ICT-middelen nog een beperkte invloed hadden op de maatschappij en men zich onvoldoende realiseerde dat informatie, waaronder informatie over personen, zich eenvoudig tot buiten de landsgrenzen kon verspreiden. Zeker met de cloud-toepassingen die we nu kennen, is het onmogelijk geworden om te traceren waar informatie over personen zich daadwerkelijk bevindt.
Op 21 oktober 2013 is de Algemene Verordening Gegevensbescherming (AVG) aangeboden aan het Europese parlement. Nadat deze op 25 mei 2016 in werking is getreden, hebben nationale overheden bedrijven en overheidsinstanties 2 jaar de tijd gegeven om aan de bepalingen van de AVG te voldoen.

Het belang van het hebben van goede bepalingen over het beschermen van persoonsgegevens is terug te voeren op andere verdragsrechtelijke en grondwettelijke bepalingen die bescherming bieden aan de persoonlijke levenssfeer, waaronder het beschermen van persoonsgegevens. Zo luidt artikel 8 van het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden:

Right to respect for private and family life
1 Everyone has the right to respect for his private and family life, his home and his correspondence.
2 There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others,

en luidt artikel 10 van de Grondwet:
1. Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer.
2. De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens.
3. De wet stelt regels inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens.

In de AVG is verder uitwerking gegeven aan het grondrecht van eerbiediging van de persoonlijke levenssfeer. Het toezicht op de naleving van deze wet ligt bij de Autoriteit Persoonsgegevens. Door recente wetswijzigingen heeft de Autoriteit aan kracht gewonnen. Zo zijn de maximale boetebedragen die de Autoriteit kan opleggen sterk verhoogd en zijn organisaties die persoonsgegevens verwerken verplicht om datalekken te melden.

Dit beleidsplan geeft gemeentelijke invulling aan de AVG. Een belangrijk issue in de Verordening is het in lijn brengen van gemeentelijke taken waarbij persoonsgegevens worden verwerkt, het doel van de verwerking, de juridische grondslag voor de verwerking en de wijze waarop met een minimum aan persoonsgegevens het doel van de verwerking kan worden bereikt.

Voldoen aan de AVG betekent dat op verschillende terreinen binnen de gemeentelijke organisatie aandacht moet zijn voor privacy. Het toverwoord in de AVG is compliance. Bedrijven en overheidsinstanties moeten aantonen dat zij inspanningen hebben gedaan om aan de wet- en regelgeving te voldoen. Om die reden zullen governance, beleid, werkprocessen en triages, bewustwording en het beheer en opslag van gegevens onder de loep genomen worden die mogelijk leiden tot aanpassing van processen of werkafspraken.

In dit beleidsplan worden allereerst een aantal begrippen en het algemene kader voor gegevensverwerking besproken. Vervolgens zal dieper ingegaan worden in hoofdstuk 5 op governance, beleid in hoofdstuk 6, werkprocessen en triages in hoofdstuk 7, bewustwording in hoofdstuk 8 en tot slot in hoofdstuk 9 op beheer en opslag van persoonsgegevens.

Voorafgaand aan dit beleidsplan is door onderzoeksbureau A3PConsultancy onderzoek gedaan naar de stand van zaken van het privacykader. Hoewel er accenten zijn aan te geven tussen de onderzoeksrapporten is er wel een gemeenschappelijke lijn te ontdekken. De aanbevelingen die uit de verschillende rapportages zijn gekomen, zijn meegenomen in dit beleidsplan en zullen ter uitwerking van dit plan in werkinstructies worden opgenomen. Zie voor het overzicht van activiteiten die uitgevoerd moeten worden na vaststelling van het beleidsplan bijlage 9.

2. Collegesamenvatting

Volgens de AVG is het college van burgemeester en wethouders (soms raad of burgemeester) verwerkingsverantwoordelijk en zijn zij gehouden aan de verordening te voldoen. Deze bestuurlijke verantwoordelijkheid zal voor de dagelijkse sturing worden belegd bij de portefeuillehouder bedrijfsvoering.

In de praktijk is privacy een issue dat op de werkvloer speelt. Uitgangspunt in dit beleidsplan is om de verantwoordelijkheid zo dicht mogelijk bij de werkvloer te organiseren door het mandateren van taken en bevoegdheden aan de teammanagers. Het mandaat behelst het geven van bevoegdheden en middelen om zelfstandig per afdeling sturing te geven aan het privacybeleid. De concernadviseurs (de functionaris gegevensbescherming, de coördinator informatieveiligheid, de strategisch informatieadviseur en de juridisch privacy-adviseur, zie verderop voor specifieke taakinhoud) bieden ondersteuning bij het inrichten van de kaders, zijn adviseurs voor technische en organisatorische kwesties, hebben een coördinerende rol in de bedrijfsvoeringscyclus en verwerken datalekken. De afdelingen zijn verantwoordelijk voor het inrichten van de interne processen, het opstellen van de juiste documenten (protocollen, verwerkingsovereenkomsten, etc) en de archivering van persoonsgegevens.

De betrokkenheid van het college bij de vormgeving van het privacybeleid bestaat uit het beoordelen van jaarplannen (uit te werken in de werkinstructies) die per afdeling wordt gemaakt en het accorderen van de inzet van middelen en het resultaat in het voorafgaande jaar. Deze verantwoording staat niet op zichzelf, maar wordt meegenomen in de reguliere P&C-cyclus van de gemeente.

De gemeente wil optimaal gebruik maken van de ruimte die de AVG biedt om persoonsgegevens te verwerken. Welke ruimte er precies is, ligt nog niet in beton gegoten. Daarom zal de gemeente binnen de lijnen van de verordening handelen, maar zal zij (als de situatie daar om vraagt) bereid zijn om risico te nemen om de grenzen van de verordening op te zoeken (bv dmv triages).

In dit beleidsplan worden onder meer de aanbevelingen uit het onderzoek van A3PConsultancy meegenomen zodat nu, samen met een groot aantal andere aspecten, een integraal beleidsplan privacy wordt gepresenteerd.

Dit beleidsplan treedt in werking met ingang van de dag na die van de bekendmaking.

Aldus vastgesteld in de collegevergadering van 11 december 2018

de secretaris de burgemeester

3. Algemeen kader voor de verwerking van persoonsgegevens

Gemeenten hebben van oudsher de beschikking over een veelheid aan persoonsgegevens. Met deze persoonsgegevens dient zorgvuldig te worden omgegaan. Vanuit de Algemene Verordening Gegevensbescherming (AVG) geldt de verplichting dat het verzamelen van persoonsgegevens steeds gekoppeld moet zijn aan een bepaald doel; de doelbinding. Binnen de gemeentelijke organisatie worden voor verschillende doelen persoonsgegevens verwerkt.

3.1. Doelbinding

Uitgangspunt in de AVG is de verwerking van de persoonsgegevens. Deze verwerkingen worden gedaan in het kader van de taakuitoefening door medewerkers. Voor deze verwerkingen geldt dat er een doel geformuleerd moet worden waarvoor zij worden verwerkt.
De AVG laat in het midden hoe die doelen geformuleerd worden, Uitgangspunt van de verordening is dat persoonsgegevens voor een welbepaald, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld. Het is een simpele aanpak om per afdeling te laten vaststellen voor welke doelen persoonsgegevens worden verwerkt bv vergunningverlening, subsidievaststelling of bepalen uitkering. Deze doeleinden worden opgenomen in het register van verwerkingen. In de praktijk wordt het toegestaan dat een doelomschrijving uit meerdere onderdelen bestaat, bijvoorbeeld in een constructie hoofddoel en subdoelen of nevendoelen. Van belang is daarbij dat deze doelstellingen onderling verenigbaar zijn. Het is ook mogelijk dat verwerkingen na melding voor andere doeleinden worden aangewend. Ook dit laatste is toegestaan, mits dit latere doel verenigbaar is met het oorspronkelijke.

In de volgende stap (nadat de doeleinden per afdeling zijn bepaald) wordt beoordeeld wat het takenpakket is van de medewerkers. Aan de hand van het takenpakket kan men beoordelen welke persoonsgegevens daarvoor verwerkt moeten worden. Voor verwerkingen die niet noodzakelijk zijn voor de uitvoering van taken, in omvang (men verwerkt gegevens van grotere groepen personen) of soort (men verwerkt meer gegevens dan noodzakelijk) kan gesteld worden dat hier geen te rechtvaardigen doel mee gediend wordt en zullen om die reden moeten worden beëindigd.

3.2. Toereikend, ter zake dienend en niet bovenmatig

Voor al deze afzonderlijke doeleinden dient vervolgens vastgesteld te worden welke persoonsgegevens hiertoe noodzakelijkerwijs wel verwerkt moeten worden. Uitgangspunt is dat het verwerken van persoonsgegevens toereikend, ter zake dienend en niet bovenmatig mag zijn. Toereikend wil zeggen dat op basis van de verwerking het juiste beeld gaat ontstaan. Ter verduidelijking; een winkelier, die een registratie bijhoudt van wanbetalers, zal een ontoereikende verwerking doen als deze niet tevens registreert of de betaling is opgeschort, omdat de klant een dispuut heeft over het product.
Ter zake dienend hangt nauw samen met het doel. Is het bijhouden door de winkelier bedoeld voor de administratie, dan kunnen de gegevens niet aangewend worden om het koopgedrag te analyseren. Bovenmatig tot slot hangt ook samen met het doel. Houdt de winkelier een registratie bij van wanbetalers voor zijn administratie, dan zal het registeren van de waarde niet bovenmatig zijn, het bijhouden van het aantal goederen mogelijk wel.

Op afdelingsniveau zal men per verwerking moeten vaststellen welke persoonsgegevens maximaal noodzakelijk zijn om het doel te kunnen bereiken (dataminimalisatie).

3.3. Vereisten van doelmatigheid, proportionaliteit en subsidiariteit

Naast de hiervoor genoemde beperkingen voor verwerking van persoonsgegevens gelden ook de eisen van proportionaliteit en subsidiariteit.
Het proportionaliteitsbeginsel houdt in dat de inbreuk op de belangen van de bij de verwerking van persoonsgegevens betrokkene niet onevenredig mag zijn in verhouding tot het met de verwerking te dienen doel. Anders gezegd; hoe verhoudt het doel van de informatieverzameling zich tegenover de schending van de persoonlijke levenssfeer van de betrokkenen. Ingevolge het subsidiariteitsbeginsel mag het doel waarvoor de persoonsgegevens worden verwerkt in redelijkheid niet op een andere, voor de bij de verwerking van persoonsgegevens betrokkene, minder nadelige wijze kunnen worden verwezenlijkt (bv het verkrijgen van de informatie uit open data).

Ook hier zal per afdeling beoordeeld moeten worden of de verwerking doelmatig is, de inbreuk op de persoonlijke levenssfeer niet zwaarder weegt als de verwerking en of de persoonsgegevens ook op een andere wijze verkregen kunnen worden.

3.4. Grondslag

Om persoonsgegevens te mogen verwerken is het noodzakelijk dat er een geldige grondslag is op basis waarvan de gegevens mogen worden verwerkt. Artikel 6 AVG geeft hiertoe een limitatieve opsomming:

- ondubbelzinnige toestemming,
- ter uitvoering van een overeenkomst,
- ter uitvoering van een wettelijke taak,
- ter vrijwaring van een vitaal belang,
- voor een goede vervulling van een publieke taak of van een taak in het kader van uitoefening openbaar gezag opgedragen aan de verwerkingsverantwoordelijke of
- vanuit gerechtvaardigde belangen.

Voor de verwerking van de persoonsgegevens is het noodzakelijk dat aansluiting gevonden kan worden bij een van deze grondslagen. Hierbij kan worden aangetekend dat de eerste grondslag enkel gebruikt wordt (ondubbelzinnige toestemming) als op grond van een van de andere grondslagen geen persoonsgegevens kunnen worden verwerkt. Als op basis van een andere grondslag (voor de gemeente Nieuwegein zal dit in de regel het uitvoeren van wettelijke taken of een goede vervulling van publieke taken zijn) het mogelijk is gegevens te verzamelen, dan wordt geen toestemming aan de betrokkene gevraagd, tenzij een wettelijke bepaling daartoe verplicht.

3.5. Verwerkingsverantwoordelijke(n) en verwerker

In de AVG wordt onderscheid gemaakt tussen verwerkingsverantwoordelijke en verwerker.
De verwerkingsverantwoordelijke is de overheidsinstantie, dienst of ander orgaan die alleen of samen met anderen het doel en de middelen voor de verwerking van persoonsgegevens vaststelt. De verwerker is de overheidsinstantie, dienst of ander orgaan die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. Voorbeelden van verwerkers zijn ICT-dienstverleners of organisaties bij wie de gemeente Nieuwegein een aantal taken laat uitvoeren.

In de relatie verwerkingsverantwoordelijke en verwerker heeft laatstgenoemde geen zeggenschap over het doel en de middelen van de verwerking. Doel en middelen worden door de verwerkingsverantwoordelijke bepaald. Om te zorgen dat de verwerker zich richt naar de instructies van de verwerkingsverantwoordelijke en kan garanderen aan de verwerkingsverantwoordelijke dat het passende technische en organisatorische maatregelen heeft genomen om de rechten van betrokkenen te beschermen, wordt een verwerkersovereenkomst gesloten. De wetgever laat het in het midden of dit een aparte overeenkomst moet zijn of dat deze geïncorporeerd kan worden in de overeenkomst tot opdracht of samenwerkingsovereenkomst.
Het template van de verwerkersovereenkomst is als bijlage 1 aan dit beleidsplan toegevoegd.

Het is ook mogelijk dat twee of meer verwerkingsverantwoordelijken gezamenlijk het doel en de middelen van de verwerking bepalen. In die gevallen is het van belang dat op een transparante wijze de onderlinge verplichtingen zijn vastgelegd in termen van overdrachtsmoment en verdeling van de aansprakelijkheden. Voor de gemeente Nieuwegein geldt dat als sprake is van een gezamenlijke verwerkingsverantwoordelijkheid dit vooraf is vastgelegd in een samenwerkingsovereenkomst aangevuld met het protocol gegevensbescherming (zie bijlage 2). Een voorbeeld waarbij persoonsgegevens van de ene verantwoordelijke naar de andere verantwoordelijke worden overgedragen is te vinden in Hoofdstuk 5 van de Wet maatschappelijke ondersteuning waar zorginstellingen als zelfstandig verantwoordelijke worden genoemd.

3.6 Technische en organisatorische beveiliging

De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. De maatregelen garanderen, rekening houdend met de stand der techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen.

In de gemeente Nieuwegein wordt aan deze eis van passende maatregelen invulling gegeven door het invoeren van de maatregelenset van de Baseline Informatiebeveiliging Gemeenten (BIG). Deze baseline is ontwikkeld door VNG/KING. Met de implementatie van deze set worden de volgende zaken beoogd:

- het invoeren van een basisniveau van informatiebeveiliging: de set is zo opgezet en ingevuld dat met invoering van de maatregelen een passend beveiligingsniveau wordt gerealiseerd voor de meeste toepassingen. Deze maatregelen betreffen niet alleen ICT-technische maatregelen maar gaan ook over huisvesting, personeelsbeleid en -werving, contractmanagement, inkoop, voorlichting en bewustwording.
- het systematisch beoordelen van informatiesystemen en -verwerking op de beveiligings- en privacyrisico's en het zo nodig treffen van specifieke maatregelen bovenop het basis-beveiligingsniveau;
- het invoeren van een proces van plannen, uitvoeren, toetsen en bijsturen (PDCA) waarbij de maatregelenset systematisch gecontroleerd wordt op effectiviteit en zo nodig aangepast wordt om het passende beveiligingsniveau blijvend te kunnen waarborgen.

Het informatiebeveiligingsproces en de maatregelenset van de BIG wordt in verschillende varianten binnen de overheid gebruikt en zijn gebaseerd op de internationale beveiligingsstandaarden. ISO 270001 en ISO 270002.

4. Governance

Om te voldoen aan de AVG zullen op bestuurlijk en ambtelijk niveau binnen de gemeente Nieuwegein een aantal organisatorische maatregelen noodzakelijk zijn. In paragraaf 4.1 en paragraaf 4.2 wordt de verdeling van bevoegdheden en verantwoordelijkheden geregeld tussen het bestuurlijke en ambtelijke niveau. Vanaf paragraaf 4.3 worden de functies benoemd die betrokken zijn bij het 'in control' brengen en houden van de gemeente Nieuwegein.

4.1. Privacy op bestuurlijk niveau

Binnen de kaders van de AVG is het college bestuurlijk eindverantwoordelijke voor de verwerking van persoonsgegevens. Deze gezamenlijke verantwoordelijkheid wordt door de gemeente Nieuwegein belegd bij een van de wethouders of de burgemeester die als vast aanspreekpunt fungeert voor privacy-issues.
In de gemeente Nieuwegein wordt er voor gekozen om de verantwoordelijkheid voor privacy-issues neer te leggen bij de portefeuillehouder informatievoorziening. Er gelden echter twee kleine uitzonderingen voor verwerkingen waarvoor de burgemeester en de gemeenteraad. Voor verwerkingen die door de burgemeester worden gedaan (denk aan verwerkingen in het kader van de openbare orde en veiligheid), is de burgemeester verantwoordelijke en voor verwerkingen die door de raad worden gedaan is de raad zelf verantwoordelijk.

Het college wil optimaal gebruik maken van de ruimte die de AVG biedt om persoonsgegevens te verwerken. De AVG stelt als ondergrens dat de overheidsinstantie compliant moet zijn en passende technische en organisatorische maatregelen dient te nemen.
Er bestaat aldus een beleidsvrijheid hoe tot het gewenste niveau van compliance te komen. Het afwegingskader daarbij is de bescherming privacy burger afgezet tegen een eigen belang van de gemeente. Voorbeelden zijn de veiligheid medewerkers borgen door persoonsgegevens niet te publiceren of bij multi-problematiek in het sociaal domein juist wel persoonsgegevens tussen hulpverleners te delen om het gezin optimaal te kunnen helpen.

Een ander aspect waarbij privacy op bestuurlijk niveau een rol speelt is het besluitvormingsproces. Het besluitvormingsproces van het college speelt zich grotendeels in de openbaarheid af. Deze openbaarheid kan gaan knellen op het moment dat er in documenten persoonsgegevens staan. Om die reden zullen persoonsgegevens zoveel mogelijk buiten collegebesluiten gehouden worden, tenzij de betrokkene toestemming heeft gegeven. Slechts in uitzonderlijke gevallen mogen persoonsgegevens zonder toestemming openbaar gemaakt worden.

Mocht het toch noodzakelijk zijn om persoonsgegevens in stukken op te nemen die bestemd zijn voor het college, dan zal vooraf een afweging worden gemaakt over de geheimhouding. Bij voorkeur is er een versie met persoonsgegevens waarop geheimhouding wordt opgelegd. In de openbare versie worden de persoonsgegevens dan onleesbaar gemaakt. Als dit niet goed mogelijk is dan kunnen de persoonsgegevens ook worden opgenomen in een geheime bijlage of kan zelfs het hele document geheim worden gehouden.
Bedenk dat persoonsgegevens niet alleen hoeven te slaan op de inwoners van de gemeente, maar ook op medewerkers. Ook hun gegevens moet zoveel mogelijk buiten verdere openbaring blijven.

Bij collegestukken zijn het collegebesluit en het voorblad openbaar (tabblad 'registreren' in het Zaaksysteem). Soms worden bijlagen bij het voorstel openbaar bekendgemaakt (bijvoorbeeld een beleidsregel).

Bij raadsstukken zijn alle stukken openbaar, tenzij er geheimhouding is opgelegd. Het beleid van de gemeente Nieuwegein is er op gericht om geen persoonsgegevens in openbare stukken op te nemen, tenzij het een bewuste keuze is het wel te doen.

4.2 Privacy op ambtelijk niveau

De feitelijke verwerking van persoonsgegevens vindt plaats binnen de ambtelijke organisatie op afdelingsniveau. De uitwerking van de eindverantwoordelijkheid die het college draagt wordt ingevuld op dit niveau. Hier worden het doel en de middelen van de verwerking bepaald zoals gebleken is uit hoofdstuk 4. Het is niet meer dan logisch dat een deel van de bevoegdheden en verantwoordelijkheden op het terrein van de privacy die ligt bij het college gemandateerd wordt naar teammanagers, zodat zij op effectieve wijze privacy in hun dagelijkse processen kunnen incorporeren.

Langs deze weg worden teammanagers primair verantwoordelijk om passende technische en organisatorische maatregelen treffen om de rechten van betrokkenen te waarborgen en de verwerking in overeenstemming te brengen met de AVG. De technische maatregelen behelzen voornamelijk het organiseren van de autorisaties. De organisatorische maatregelen hebben betrekking op het bewust omgaan met persoonsgegevens en het treffen voorzieningen waardoor medewerkers hun taken kunnen blijven uitvoeren.

De verantwoordelijkheid van de teammanagers op privacygebied is gekoppeld aan mandaten vanuit het college met daarin bevoegdheden en middelen. Hierbij kan worden gedacht aan:
- inrichten van de werkprocessen in overeenstemming met AVG,
- bepalen van het doel en middel van de verwerking,
- alloceren middelen in termen van menskracht en geld voor onder andere bewustwordingssessies,
- bepalen van (mede)verantwoordelijkheid voor de verwerking,
- voorbereiden van verwerkingsrelaties, protocollen en verwerkingsovereenkomsten opstellen (al dan niet als onderdeel van de samenwerkingsovereenkomst),
- ondertekenen van protocollen en verwerkingsovereenkomsten
- technische infrastructuur voor de verwerkingen,
- archivering,
- inzetten privacy impact assessment (PIA) of soortgelijke instrumenten om de privacy te toetsen,
- waarborgen rechten betrokkenen,
- melden van verwerkingen bij de functionaris gegevensbescherming (FG) en
- melden datalekken en andere incidenten

De teammanagers dragen er ook zorg voor dat medewerkers op de afdeling gehouden zijn tot geheimhouding van de persoonsgegevens waar zij kennis van nemen. Voor de ambtenaren die in vaste dienst zijn bij de gemeente geldt de eedsaflegging. Voor personen die niet in dienst zijn van Nieuwegein (bv. Leden van de bezwarencommissie) of die tijdelijk worden ingehuurd geldt dat zij een geheimhoudingsverklaring moeten tekenen. Het template van de geheimhoudingsverklaring is opgenomen in bijlage 3.

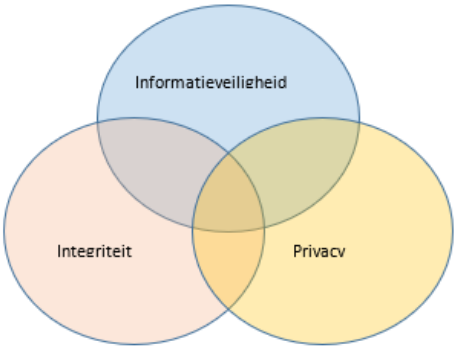
Om de portefeuillehouder betrokken te houden en om, samen met het college, de rol van verwerkingsverantwoordelijke in het kader van de privacy waar te maken zal in de PDCA-cyclus (zie par 7.7) het thema privacy worden meegenomen in het programmaonderdeel bedrijfsvoering in de jaarrekening. Ter uitvoering van dit beleidsplan zal een implementatie- en onderhoudsplan geschreven worden waarin dit thema verder zal worden uitgewerkt.

4.3 Samenhang tussen privacy en informatieveiligheid

Een belangrijk thema voor privacy is de wijze waarop de gemeente Nieuwegein persoonsgegevens heeft beveiligd. Bij het beveiligen van persoonsgegevens wordt sterk geleund op bestaande technische mogelijkheden. Naast techniek is de gemeente ook afhankelijk van menselijk gedrag.

Om het menselijk gedrag zo veel mogelijk te sturen zal, en dit wordt ook genoemd in artikel 25 AVG, bij het ontwikkelen van software rekening gehouden worden met de 'privacy by design' en de 'privacy by defaults'.
Voor wat betreft het ontwerpen en toepassen van software (design) worden maatregelen getroffen waarbij de hoeveelheid betrokken persoonsgegevens wordt geminimaliseerd en waar mogelijk zelfs gepseudonimiseerd. Waar het gaat om de standaardinstellingen (defaults) wordt er voor gekozen voor instellingen waarbij enkel door actieve handelingen persoonsgegevens worden verwerkt.

Door toepassen van techniek, het beïnvloeden van menselijk gedrag en als uitgangspunt dataminimalisatie te nemen grijpen informatieveiligheid, privacy en integriteit in elkaar:



Deze onderwerpen overlappen elkaar deels. Deze ontwikkeling waarbij techniek, menselijke gedrag en het beschermen van persoonsgegevens meer verweven raken met elkaar wordt ook uitgedragen in de andere lekstroomgemeenten, waardoor (mocht dat gewenst zijn) in de toekomst op meerdere terreinen en waarbij deze aspecten een rol spelen, gemakkelijker worden samengewerkt.

4.4 Functionaris gegevensbescherming

Op grond van artikel 37 AVG wordt een functionaris gegevensbescherming (FG) aangewezen. De verwerkingsverantwoordelijke draagt hierbij zorg dat de FG aangewezen wordt op grond van zijn professionele kwaliteiten en, in het bijzonder, zijn deskundigheid op het gebied van wetgeving en de praktijk inzake gegevensbescherming en zijn vermogen om de taken die met zijn functie samenhangen, genoemd in artikel 39 AVG, te vervullen.

De verwerkingsverantwoordelijke is op grond van artikel 37 AVG gehouden om de contactgegevens van de FG bekend te maken en mede te delen aan de Autoriteit Persoonsgegevens (AP). Binnen de gemeente Nieuwegein valt de FG formatief onder bedrijfsvoering.

De FG heeft een informerende en adviserende rol aan de organisatie over verplichtingen die voortvloeien uit de verordening. Daarnaast ziet de FG toe op de naleving van de verordeningsbepalingen en draagt de functionaris zorg voor de privacy-audits. Tot slot fungeert de FG als eerste aanspreekpunt voor de Autoriteit Persoonsgegevens.

Van resultaten uit audits en overige bevindingen doet de FG rechtstreeks verslag aan het college van burgemeester en wethouders van de gemeente.

4.5 Coördinator rechtsbescherming

In geval van een schending dan wel uitoefening van rechten van betrokkenen (zie paragraaf 6.1) moet een betrokkene, los van andere juridische middelen, zich kunnen wenden tot de gemeente als verwerkingsverantwoordelijke.

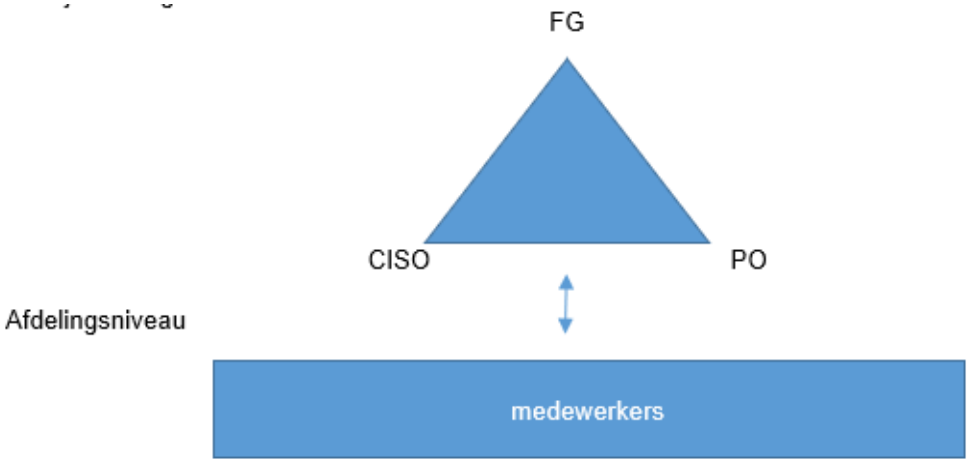
Binnen de gemeente Nieuwegein is een coördinator aangewezen waar verzoeken en bezwaren (ex artikel 21 AVG) kunnen worden ingediend. De coördinator bewaakt de termijn en draagt er zorg voor een goede afhandeling van het verzoek of bezwaar.

4.6 Overige functies in kader van privacy

Buiten de in de AVG met naam genoemde functie van FG houden zich binnen de gemeente Nieuwegein ook anderen zich nadrukkelijk bezig met de dagelijkse praktijk rond privacy.

Organisatorisch wordt op twee niveaus uitwerking gegeven aan het privacybeleid; bedrijfsvoerings- en afdelingsniveau.
Op bedrijfsvoeringsniveau vertaalt het zich in een driehoek bestaande uit FG, Chief information and securityofficer (CISO) en de privacyoffice (PO). Uiteraard kunnen dit volwaaridge functies zijn, maar evengoed ook rollen die medewerkers naast hun dagelijks werk doen. De PO bestaat uit de coördinator informatieveiligheid, de strategisch informatieadviseur, de juridisch privacy-adviseur en de procesondersteuner PO. Het doel van de driehoek is om centrale kennisbank te hebben rond het thema privacy en beveiliging. Alle issues die leven op de werkvloer worden door de driehoek in behandeling genomen en centraal opgeslagen, waarna ze voor iedereen toegankelijk zijn.

Bedrijfsvoeringsniveau



Naast toezicht op naleving AVG ziet de FG tevens toe op informatieveiligheid, waarmee er op het gebied van informatieveiligheid een goede functiescheiding is gemaakt tussen CISO en FG. Hierbij zorgt de coördinator informatieveiligheid er voor dat de juiste en passende beveiligingsmaatregelen gekozen, geïmplementeerd en geëvalueerd worden. De FG ziet toe op de werking van het proces en de maatregelen en brengt hier verslag van uit aan het management en bestuur.

Binnen de gemeente Nieuwegein is de PO verantwoordelijk voor het vormgeven en actualiseren van het gemeentelijke privacy-beleid, het doen van organisatorische aanpassingen en draagt hij zorg dat documenten en andere beslissingen voldoen aan de privacywetgeving. Verder houdt de PO het register van verwerkingen en het register van verwerkers bij. Tot slot fungeert de adviseur als aanspreekpunt voor vragen over toepassing wet- en regelgeving inzake privacy.

Nu teammanagers nadrukkelijk verantwoordelijkheid dragen voor de verwerkingen die op hun afdeling wordt verricht, is het zeker in de beginfase wenselijk een persoon vrij te maken voor het thema privacy binnen dat team. De taken die deze medewerker verricht hangen samen met hetgeen staat opgesomd in paragraaf 5.2.
Zo zal deze medewerker binnen de afdeling als aanspreekpunt belast worden met de dagelijkse praktijk fungeren en werkinstructies schrijven. Uiteraard kan deze medewerker voor ingewikkelder vraagstukken ondersteuning vragen bij de driehoek.

4.7 Externe relaties/verwerkersovereenkomst

Het verwerken van persoonsgegevens is geen doel op zich, maar zal in het teken staan van een ander gerechtvaardigd doel dat met die verwerking zal worden bereikt (het verlenen van zorg, het houden van toezicht of het uitbetalen van salarissen). Ten behoeve van dat andere doel zullen vaak persoonsgegevens van elders betrokken worden of zullen persoonsgegevens worden overgedragen aan anderen.

Bij het verwerken van persoonsgegevens elders worden in de AVG twee mogelijke samenwerkingsconstructies genoemd; gezamenlijke verwerkingsverantwoordelijkheid en de verwerking namens de verwerkingsverantwoordelijke. Buiten deze twee in de AVG genoemde samenwerkingsconstructies is ook nog denkbaar dat de persoonsgegevens die door de gemeente worden verwerkt worden overgedragen naar een andere verwerkingsverantwoordelijke (denk bij het

sociaal domein aan een zorginstelling waarbij de overdracht aan de andere verwerkingsverantwoordelijke bij wet geregeld is).

A gezamenlijke verwerkingsverantwoordelijkheid

Van een gezamenlijk verwerkingsverantwoordelijkheid is sprake wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen. In dat geval stellen zij op transparante wijze hun respectieve verantwoordelijkheden voor de nakoming van hun verplichting uit hoofde van de AVG vast, met name met betrekking tot de uitoefening van rechten van betrokkenen en het verstrekken van informatie aan hen. De relatie tussen de verwerkingsverantwoordelijken onderling wordt bestendigd door middel van een protocol. In bijlage 2 bij dit beleidsplan is een voorbeeldprotocol gevoegd.

B verwerkingsverantwoordelijke en verwerker

Wanneer een verwerking, namens een verwerkingsverantwoordelijke wordt verricht, en de verwerker geen zeggenschap heeft over doel en middel van de verwerking, dan doet de verwerkingsverantwoordelijke uitsluitend een beroep op verwerkers die afdoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen bieden opdat de verwerking voldoet aan de eisen van de AVG.

De gemeente blijft als verwerkingsverantwoordelijke (mede-)aansprakelijk voor de geschonden rechten van betrokkenen door nalatigheden van de kant van de verwerker. Om de verantwoordelijkheid en aansprakelijkheden goed uit elkaar te houden zal de gemeente in deze situaties gebruik maken van verwerkersovereenkomsten. Het gebruik van verwerkingsovereenkomsten is een verplichting die voortvloeit uit de AVG. De verwerkingsovereenkomst is vormvrij en kan dus ook geregeld worden in de bovenliggende overeenkomst tot samenwerking, opdracht, dienstverlening etc. Om een beeld te hebben van de wijze waarop de relatie tussen verwerkingsverantwoordelijke en verwerker moet worden vormgegeven is een template verwerkersovereenkomst als bijlage 1 bij dit beleidsplan opgenomen.

C Overdracht van persoonsgegevens aan een andere verwerkingsverantwoordelijke

Daar waar het gaat om een overdracht van de persoonsverwerking (bijvoorbeeld in de vorm van bestanden) aan een andere verwerkingsverantwoordelijke zal er na overdracht geen gebondenheid meer zijn van de gemeente Nieuwegein. De inspanning van de gemeente Nieuwegein blijft hier beperkt tot het vaststellen of de ontvangende partij daadwerkelijk verwerkingsverantwoordelijke is. (Een dergelijk situatie doet zich vaak voor in het sociaal domein waar zorginstellingen, SVB, AMHK in de wet als verwerkingsverantwoordelijke zijn aangewezen.) Ook in deze situatie is het overdrachtsprotocol als genoemd in bijlage 2 een passende oplossing.

5 Privacybeleid

In de AVG worden een aantal generieke normen gesteld waar de verwerkingsverantwoordelijke inhoud aan moet geven. Door het normenkader zelf vorm te geven kan de verwerkingsverantwoordelijke eigen accenten aanbrengen of beleidsuitgangspunten toevoegen. De gemeente Nieuwegein hecht er waarde aan dat de persoonsgegevens die aan haar zijn toevertrouwd alleen gebruikt worden voor de doeleinden waarvoor zij zijn gegeven. Dit wordt anders als de gegevensbescherming een gevaar oplevert voor hulpverlening en veiligheid. De gemeente zoekt in dergelijke gevallen de grenzen van de privacywetgeving op als daarmee een groter gevaar kan worden afgewend dat kan ontstaan als medewerkers en andere hulpverleners langs elkaar heen werken. Beslissingen die in dat verband genomen worden zullen duidelijk gemotiveerd worden.

Het beleid van de gemeente is ook gericht op transparantie en bewustwording. Zowel intern als extern zal er een open communicatie zijn over de wijze van verwerking van persoonsgegevens.

Binnen het thema beleid verdienen vijf aspecten nadere invulling; rechten van betrokkenen, rechten personeelsleden, geautomatiseerde verwerkingen, datalekken en bewaren van persoonsgegevens.

5.1 Rechten van betrokkenen

Binnen de AVG worden verschillende rechten toegekend aan betrokkenen opdat zij de regie kunnen voeren op de persoonsgegevens die bij de gemeente Nieuwegein worden verwerkt.
Het gaat om de volgende rechten:

1. Recht op informatie (artikel 12 AVG)

Er dienen maatregelen genomen te worden zodat de betrokkene op een beknopte, transparante, begrijpelijke en in gemakkelijk toegankelijke vorm informatie kan verkrijgen over zijn persoonsgegevens en geïnformeerd wordt over verwerkingsactiviteiten.
Het verstrekken van informatie geschiedt onverwijld en in ieder geval binnen een maand na ontvangst van het verzoek.

2. Recht op inzage (artikel 15 AVG)
Betrokkene heeft het recht uitsluitsel te krijgen over het al dan niet verwerken van hem betreffende persoonsgegevens en om inzage te verkrijgen van die persoonsgegevens en de volgende informatie:
- verwerkingsdoelen,
- betrokken categorieën van persoonsgegevens,
- ontvangers of categorieën ontvangers aan wie persoonsgegevens worden verstrekt,
- duur van de verwerking en opslag,
- het recht op rectificatie en gegevenswissing,
- het recht om een klacht in te dienen bij de toezichthoudende autoriteit,
- (indien gegevens niet bij betrokkene worden verzameld) informatie over de bron van de gegevens en
- het bestaan van geautomatiseerde besluitvorming, het belang en de te verwachten gevolgen voor betrokkene.

3. Recht op rectificatie (artikel 16 AVG en 19 AVG)
Betrokkene heeft het recht dat onjuiste persoonsgegevens onverwijld worden gerectificeerd en dat onvolledige gegevens worden aangevuld. De verwerkingsverantwoordelijke stelt iedere ontvanger op de hoogte van de recificatie of aanvulling.

4. Recht op gegevenswissing (artikel 17 AVG en 19 AVG)
Onder omstandigheden heeft betrokkene het recht dat zijn gegevens zonder onredelijke vertraging worden gewist. Per verwerking zal moeten worden bepaald of gegevenswissing mogelijk is. De verwerkingsverantwoordelijke stelt iedere betrokkene op de hoogte van de wissing.

5. Recht op beperking van de verwerking (artikel 18 AVG)
Onder omstandigheden heeft betrokkene het recht om een beperking van de verwerking te verkrijgen, indien de juistheid van de persoonsgegevens worden betwist, de verwerking onrechtmatig is, de persoonsgegevens niet meer noodzakelijk zijn voor het doel waarvoor ze zijn verwerkt of indien betrokkenen bezwaar heeft gemaakt tegen de verwerking

6. Recht op overdraagbaarheid (artikel 20 AVG)
Betrokkene heeft het recht om zijn persoonsgegevens in een gestructureerde, gangbare en machineleesbare vorm te verkrijgen en het recht deze gegevens over te dragen aan een andere verwerkingsverantwoordelijke.

7. Recht op bezwaar (artikel 21 AVG)
Betrokkene heeft steeds het recht bezwaar te maken tegen de verwerking. De verwerkingsverantwoordelijke staakt de verwerking, tenzij er dwingende gerechtvaardigde gronden zijn die zwaarder wegen dan de belangen van de betrokkene.

8. Recht om niet onderworpen te worden aan een enkel op geautomatiseerde verwerking gebaseerd besluit (artikel 22 AVG).(Profiling)
Betrokkene heeft het recht om niet onderworpen te worden aan een enkel op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft.

9. Klachtrecht en schadevergoedingsrecht (artikel 77 AVG en artikel 82 AVG)
Betrokkene heeft het recht een klacht in te dienen bij de toezichthoudende autoriteit en het recht op een vergoeding van materiële of immateriële schade ten gevolge van inbreuk op bepalingen AVG en waarvoor de verwerkingsverantwoordelijke aansprakelijk is jegens de betrokkene.

Het uitgangspunt voor de gemeente Nieuwegein is dat gestreefd wordt naar een maximale transparantie tegenover de betrokkene waar het gaat om de 'eigen' persoonsgegevens.
Waar het gaat om het recht op informatie zullen de gemeenten in zijn algemeenheid op de website (privacy statement; zie bijlage 4) en in de correspondentie betrokkenen wijzen op het feit dat persoonsgegevens worden verwerkt en dat betrokkenen een aantal rechten hebben op grond van de AVG. Inhoudelijk worden deze verzoeken en bezwaren door de coördinator rechtsbescherming (zie paragraaf 5.4) begeleid. Om de afhandeling hiervan te vergemakkelijken zullen standaardbrieven worden gehanteerd.

5.2 Rechten personeelsleden

In het licht van de AVG zijn de gegevens van medewerkers eveneens gegevens van betrokkenen en verdienen om die reden aandacht.

De komst van de AVG biedt ook een goede gelegenheid om de verwerking van persoonsgegevens van medewerkers van de gemeente eens tegen het licht te houden. Er zijn twee situaties waarbij persoonsgegevens van medewerkers kunnen worden geopenbaard, via raad- en collegebesluiten of via persoonlijke correspondentie.

Omdat het hier om het recht van medewerkers gaat en de taakuitvoering van een gemeente divers en soms complex is pas het niet hier één richtinggevende standpunt over in te nemen. In de implementatie moet per onderdeel steeds een zorgvuldige afweging worden gemaakt waarbij ook de inbreng van medewerkers over hun bescherming moet worden meegewogen. Uitgangspunt is wel dat medewerkers niet individueel de afweging kunnen maken. Het college verzoekt de directie dit langs het implementatieplan op te nemen met de ondernemingsraad. Qua bestuurlijke portefeuille is dit deel een verantwoordelijkheid van de portefeuillehouder P&O.

In geval sprake is van Wob-verzoeken kunnen de namen van medewerkers achterwege blijven. Uit artikel 10, eerste lid onder d Wob vloeit dit al voort. In het kader van dit beleidsplan wordt artikel voornoemde regel gevolgd met de aanvulling dat er snel sprake zal zijn van een aantasting van de persoonlijke levenssfeer. Voor degene die Wob-verzoeken afhandelt betekent dit een extra alertheid.

5.3 Geautomatiseerde verwerkingen en cameratoezicht

Onder geautomatiseerde verwerkingen wordt verstaan het met gebruikmaking van elektronische middelen gegevens verwerken. Een voorbeeld is profilering. Door het bezoeken van bepaalde gemeentelijke websites door betrokkenen kunnen bepaalde persoonlijke voorkeuren worden vastgelegd en geanalyseerd en kan de gemeente aan de bezoeker bepaalde gerichte producten of diensten aanbieden. Door de gemeente Nieuwegein wordt hier geen gebruik van gemaakt.

Voor onderzoeken zal de gemeente, indien dat in het kader van het onderzoek gewenst is, gebruik maken van Big data en tracking wanneer de aldus verzamelde gegevens niet te herleiden zijn tot een natuurlijke persoon. In die gevallen waarin de gemeente gebruik maakt van Big data onderzoeken en tracking, dan zal zij daarover vooraf informatie verstrekken op de gemeentelijke website.

Protocol cameratoezicht is nog niet toegevoegd is omdat nog bestuurlijk afgestemd moet worden.

5.4 Datalekken

Van een datalek is sprake bij een onrechtmatige verwerking en als persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens zouden mogen hebben. Een datalek is het gevolg van een beveiligingsincident. In de meeste gevallen gaat het om uitgelekte computerbestanden, al kan een verloren uitgeprinte klantenlijst evengoed een datalek vormen. Andere voorbeelden: cyberaanvallen (incl. DDos), e-mail verzonden naar verkeerde adressen, onderschepte e-mails, niet aangekomen post, gestolen laptops of bedrijfstelefoons, afgedankte niet-schoongemaakte computers en verloren usb-sticks.

Beveiligingsincidenten worden nu al gemeld door medewerkers of verwerkers bij de CISO van de gemeente. De CISO maakt een analyse of het beveiligingslek mogelijk ook een datalek is. Bij een vermoeden van een datalek wordt de FG gewaarschuwd. Gelet op het feit dat het al sinds 1 januari 2016 verplicht is om datalekken te melden bij de Autoriteit heeft de gemeente Nieuwegein inmiddels een werkinstructie meldplicht datalekken zal dit beleidsthema hier verder onbesproken blijven. Verwezen wordt naar bijlage 5.

5.5 Bewaren van persoonsgegevens

Persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk is voor de verwerking. Voor wat betreft het bewaren van persoonsgegevens geldt voor de gemeente Nieuwegeintwee regiems, het wettelijke regiem en het niet wettelijke regiem.
Voor sommige verwerkingen van persoonsgegevens geldt dat deze persoonsgegevens op grond van de Archiefwet of andere materiële wetten een minimale termijn bewaard moeten blijven. Een voorbeeld is het jeugdhulpdossier dat 15 jaar nadat de jeugdhulp beëindigd is bewaard moet blijven. De AVG gaat niet in op de wettelijke termijnen die bestaan of in de toekomst zullen ontstaan.
Voor die verwerkingen waarvoor geen wettelijke termijn geldt, bv. de gemeente heeft een onderzoek gedaan naar relschoppers in de wijk X, dat de verwerkte persoonsgegevens worden vernietigd zodra de verwerking niet meer noodzakelijk is ter bepaling door de teammanager en wordt vastgelegd in het verwerkingsregister.

Voor wat betreft het archiveren van persoonsgegevens zoekt de gemeente Nieuwegeinaansluiting bij artikel 89 AVG. Archiveren in het algemeen belang is mogelijk, mits passende maatregelen zijn getroffen om de betrokkenen te beschermen. Vaststaat dat persoonsgegevens die voor een gerechtvaardigd doel zijn verwerkt ook verwerkt mogen worden in de zin van archiveren (verenigbaar doel). Wel zal men opnieuw moeten beoordelen of verdere dataminimalisatie mogelijk is. Is dataminimalisatie mogelijk door ontkoppeling van de persoonsgegevens met de overige gegevens, dan zal daar voor gekozen worden. Als tussenvorm is het mogelijk om in het kader van archivering te werken met pseudonimiseren.

Om Archiveren in goede banen te leiden zal er apart onderzoek worden gedaan naar het opslaan van persoonsgegevens in gemeentelijke archieven. De insteek zal zijn om vanuit het register van verwerkingen die bestanden te selecteren waarbij een afwijkend archiefregiem geldt en hiervoor separaat instructies te maken.

6 Werkprocessen

In dit hoofdstuk staat de vraag centraal op welke wijze de gemeente Nieuwegein de verwerking van persoonsgegevens vorm geeft in bedrijfsprocessen en op welke wijze medewerkers gebruik kunnen maken van databases. In 6.1 zal het kader geschetst worden hoe verwerking van persoonsgegevens in de bedrijfsprocessen moet worden ingebed. In 6.2 wordt een bijzondere toepassing van verwerking van persoonsgegevens besproken waar hulpverleners en veiligheidsadviseurs mee te maken hebben in de dagelijks praktijk. 6.3 gaat dieper in op triages die hoofdzakelijk voorkomen in het sociaal domein. 6.4 bespreekt het gebruik van BSN (een persoonsgegeven ogv Uitvoeringswet AVG). In 6.5 wordt dieper ingegaan op het verwerkingenregister dat door de gemeente moet worden aangelegd en op basis waarvan de FG zijn toezicht kan effectueren. In paragraaf 6.6 wordt besproken hoe met Privacy Impact Assessments (PIA's) privacyrisico's van gegevensverwerkingen in beeld gebracht worden en hoe deze vervolgens te vertalen in het werkproces. In de laatste paragraaf komt de PDCA-cyclus aan de orde.

6.1 Inbedding in primaire processen

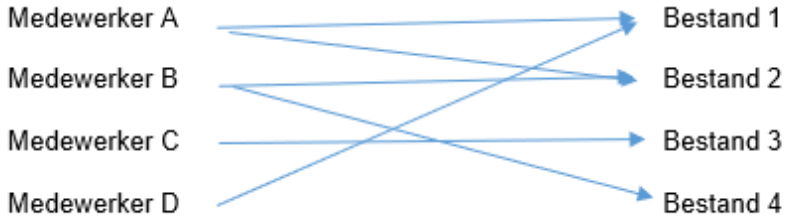
De AVG eist dat voor gemeente Nieuwegeinverwerking van persoonsgegevens de beginselen inzake verwerking van persoonsgegevens in acht genomen zijn. Deze beginselen vloeien voort uit artikel 5 en 6 AVG (zie voor verdere uitleg H3 van dit beleidsplan).

Zo moet de verwerking van persoonsgegevens kunnen steunen op welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Voor werkprocessen binnen de gemeente Nieuwegein betekent dit dat bij verwerkingen een geldige reden moet zijn om de inperking van het grondrecht privacy te rechtvaardigen. Ontbreekt een dergelijke reden, dan is de verwerking illegaal en zal zij moeten worden beëindigd.

Concreet betekent een en ander dat er zicht moet zijn op de taken van (groepen) medewerkers waarbij persoonsgegevens worden verwerkt. Aan de hand van het overzicht van gegevensverwerkingen van de medewerkers zullen door het afdelingsmanagement gerechtvaardigde doeleinden moeten worden geformuleerd om de verwerking voort te kunnen zetten. Nadat doeleinden zijn geformuleerd is het noodzakelijk om te beoordelen welke persoonsgegevens ten minste verwerkt moeten worden om dat doel te kunnen bereiken. Persoonsgegevens die bovenmatig zijn kunnen buiten de verwerking blijven.

De volgende stap is dat aansluiting gevonden wordt bij een van de grondslagen uit artikel 6 AVG (zie tevens paragraaf 3.4). Voor de gemeente Nieuwegein zal gaan gelden dat veel verwerkingen als grondslag de goede vervulling van een publieke taak kennen. In bijzondere gevallen zal een beroep op een van de andere grondslagen, ten finale mogelijk toestemming, gedaan moeten worden.

Schematische weergave van verdeling takenpakket en toegang tot gegevensbestanden:



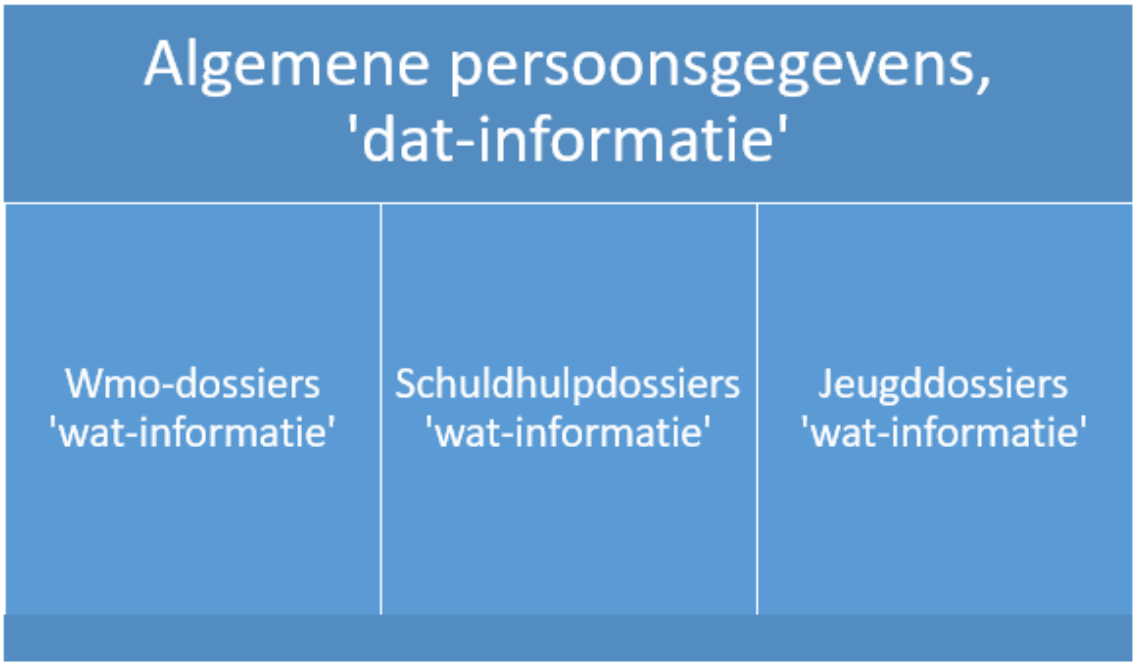
Uitgangspunt zijn de taken die door de medewerkers worden uitgevoerd. Deze taken vloeien voort uit functieomschrijvingen. Om in bestanden verwerkingen uit te kunnen voeren zal men toegang tot die bestanden moeten hebben door middel van autorisatie (waar het om digitale bestanden gaat). Het is belangrijk om steeds meerdere mensen te autoriseren voor dergelijke bestanden om te voorkomen dat een situatie ontstaat dat niemand bij de bestanden kan. Het is niet aannemelijk dat de teammanager per definitie toegang moet hebben, dit is ook weer afhankelijk van zijn takenpakket.

6.2 Samenwerken met collega's

Binnen de gemeentelijke organisatie hebben medewerkers een takenpakket die bepalend is voor de toegang tot bestanden. Binnen takenpakketten kan er wel een onderscheid zijn in de diepte waarmee men toegang moet hebben tot de bestanden. Met name in het sociaal domein (mogelijk ook elders) kan het wenselijk zijn dat veel medewerkers een kleine hoeveelheid persoonsgegevens kunnen inzien en dat vervolgens een paar medewerkers de totale omvang van de persoonsgegevens (vastgelegd in bv een dossier) mogen inzien.
Ter verduidelijking. De KCC-medewerker moet de naw-gegevens hebben om door te kunnen verwijzen naar de juiste medewerker, de WMO-consulent moet naast naw-gegevens ook de dossierinformatie kunnen inzien om optimale hulp te kunnen verlenen.

Het verdelen van de diepte van de toegang wordt langs de lijn 'dat-wat' gelegd. Medewerkers (zoals voornoemde KCC-medewerker) kunnen geautoriseerd worden voor de dat-informatie (men weet dat er wat speelt om vervolgens door te kunnen verwijzen) en medewerkers (zoals voornoemde WMO-consulent) die geautoriseerd worden voor de dat-wat-informatie. Zij kunnen het gehele dossier inzien.

Autorisatieschema:



6.3 Triage

Aparte aandacht verdient het proces rond de triage. Uitgangspunt in hulpverlening is om zoveel mogelijk te handelen vanuit 1Gezin,1Plan,1Regisseur (1G1P1R). Triage speelt op casusniveau en vraagt van de medewerker om een professionele inschatting te maken wat de ernst van de problematiek is en welke

verwerking van persoonsgegevens daarbij wenselijk is. Met name bij een multi-probleemsituaties in het sociaal domein kan er opschaling nodig zijn waardoor meer persoonsgegevens worden verwerkt of persoonsgegevens met anderen worden gedeeld. Dit is te rechtvaardigen om te voorkomen dat privacy in de weg gaat staan aan een effectieve hulpverlening. Triage doorsnijdt aldus de 1G1P1R-gedachte.

Medewerkers bepalen per casus het doel waarvoor de gegevensverwerking noodzakelijk is voor optimale hulp. Daarnaast bepalen zij of er niet bovenmatig gegevens worden verwerkt of dat gegevens niet op een andere, minder ingrijpende wijze, kunnen worden verwerkt. Van belang is dat deze afweging door de medewerker wordt vastgelegd. Triagemomenten worden benoemd in het werkproces. Gaandeweg het hulpverleningsproces aan het gezin en waarbij meerdere hulpverleners betrokken zijn zullen vanuit deze triage overlegmomenten worden georganiseerd waarin persoonsgegevens worden uitgewisseld. Deze overlegmomenten worden gedocumenteerd, zodat het voor de FG duidelijk is welke uitwisseling van persoonsgegevens heeft plaatsgevonden.

De grondslag voor triage is voor de gemeente Nieuwegein het uitvoeren van een publiekrechtelijke taak. Dit betekent concreet dat het toepassen van triage beperkt is tot die werkprocessen waarbij het uitwisselen van persoonsgegevens binnen en buiten de eigen organisatie terug te voeren is op het uitvoeren van een dergelijke taak. Medewerkers van de gemeente Nieuwegein moeten er daarbij rekening mee houden dat het delen met professionele hulpverleners samenhangt met diens geheimhoudingsplichten (en dus niet alles gedeeld kan worden).
In een stappenplan wordt uiteengezet wat de randvoorwaarden zijn bij integrale gegevensverwerking in het sociaal domein (zie bijlage 6).

6.4 Gebruik Burgerservicenummers

Er is nog veel onduidelijkheid over het gebruik van het BSN nummer in werkprocessen. De regel is dat overheidsorganisaties het BSN mogen gebruiken om hun taak uit te voeren, mits het BSN hierbij noodzakelijk is. Organisaties buiten de overheid mogen het BSN alléén gebruiken als dit in de wet staat. En dan nog alleen voor de doelen die in de wet staan, dus niet zomaar overal voor.
Zo liet een kinderdagverblijf ouders inloggen op een online ouderportaal met hun BSN. Dat mag niet. Kinderdagverblijven mogen weliswaar naar het BSN van ouders vragen, maar zij mogen dit vervolgens alleen gebruiken voor de kinderopvangtoeslag.

Het voorbeeld van het kinderdagverblijf komt ook regelmatig terug in gemeentelijke processen. Zo mag de gemeente een BSN niet gebruiken als briefkenmerk of dossiernummer. De gemeente mag ook niet standaard om BSN vragen of laten te vermelden in brieven die u naar de gemeente stuurt.

Het is vaak niet nodig dat de gemeente een BSN opneemt in aan burgers gerichte brieven. En dan mag het ook niet. Wel kan de gemeente vragen om een BSN te vermelden bij bepaalde verzoeken of vragen aan de gemeente. Maar dat mag alleen als zo'n verzoek of vraag gaat over een persoonlijke situatie waarbij de medewerker duidelijk wil vaststellen om wie het gaat.
Heeft u een algemene vraag aan de gemeente, bijvoorbeeld over afval? Dan hoeft u uw BSN niet te vermelden.

Om BSN in goede banen te leiden zal er apart onderzoek worden gedaan naar het verwerken van persoonsgegevens met BSN of aan de hand van BSN. De insteek zal zijn om vanuit het register van verwerkingen die bestanden te selecteren waarbij BSN in het spel is en hiervoor separaat een PIA op uit te voeren.

6.5 Verwerkingenregister

Zoals in het hoofdstuk Governance reeds is aangegeven ligt de ambtelijke verantwoordelijkheid voor het verwerken van persoonsgegevens bij de teammanager. Zij brengen in beeld en bewaken het overzicht van de gegevensverwerkingen die op de afdeling plaatsvinden.
Kader van het overzicht wordt gevormd door artikel 30 van de AVG. Zo zal onder meer vastgesteld moeten zijn dat de verwerking een gerechtvaardigd doel kent en gebaseerd is op een rechtmatige grondslag. Uiteindelijke levert dit het volgende plaatje op:

Verwerkingsregister									
Taakverantwoordelijke	Naam verwerking/proces	Doel verwerking	Betrokkenen	Persoonsgegevens	Bijzondere persoonsgegevens	Ontvangers	Grondslag	Bewaartermijnen	Beschrijving beveiligingsmaatregelen

Het overzicht van gegevensverwerkingen wordt geleverd aan de PO die een register houdt van alle verwerkingen van persoonsgegevens binnen de gemeente Nieuwegein. Aan de hand van het register van verwerkingen zal de FG toezicht houden op het totaal aantal verwerkingen binnen de gemeente.

6.6 Privacy Impact Assessment

Met het uitvoeren van een Privacy Impact Assessment (PIA) wordt inzicht verkregen in de privacyrisico's van een nieuwe dienst of een nieuw product. Maar ook het hergebruik van reeds verwerkte data voor nieuwe toepassingen is een voorbeeld waarvoor een PIA een duidelijk inzicht geeft aan de betrokken risico's.

Een PIA wordt bij voorkeur in een zo vroeg mogelijk stadium van het ontwerpproces uitgevoerd, zodat uitkomsten van de PIA nog meegenomen kunnen worden en invulling gegeven kan worden aan 'privacy by design'. Een PIA kan ook in een later stadium uitgevoerd worden, omdat de meeste processen 'doorontwikkeld' worden en ook later nog privacyrisico's kunnen worden ingedamd.

Het is niet noodzakelijk om voor alle processen waarbij persoonsgegevens worden verwerkt een PIA uit te voeren. Om die reden is er een onderscheid aangebracht en zullen in 2018 enkel PIA's worden uitgevoerd in geval van nieuwe verwerkingen van persoonsgegevens en verwerkingen waarbij sprake is van een grote verzameling van persoonsgegevens of een verzameling met bijzondere categorieën van persoonsgegevens. Een selectie van verwerkingen waarvoor een PIA wordt georganiseerd vloeit voort uit het verwerkingenregister als genoemd in paragraaf 7.5.

In eerste aanleg zullen de PIA's worden uitgevoerd onder leiding van de kwartiermaker FG en later door de FG.

6.7 PDCA-cyclus

Privacy is niet een op zichzelf staand thema. Het vraagt om een voortdurende aandacht en moet ook goed ingebed worden in de organisatie. De primaire verantwoordelijkheid om de bescherming persoonsgegevens op de juiste wijze in te bedden in de organisatie ligt bij de afdelingshoofden. Zij krijgen de middelen (zie paragraaf 5.2) om handen en voeten te geven aan de uitvoering van het privacybeleid op hun afdeling. Vanuit die vertaalslag van strategisch beleidsplan naar operationele uitvoering zal ook het succes van het plan blijken.

Het is uiteindelijk ook de bedoeling om ten aanzien van het thema privacy en informatieveiligheid gezamenlijke streefdoelen af te spreken. Doelen zouden kunnen zijn, terugdringen datalekken, heldere autorisaties, optimale beveiliging, om maar een paar voorbeelden te benoemen. Om het succes te kunnen meten kan gedacht worden aan benchmarking met de andere lekstroomgemeenten.
.

7 Bewustwording

7.1 Veilig omgaan met informatie en persoonsgegevens

Het is belangrijk dat privacy, informatieveiligheid en integriteit niet alleen leeft bij een aantal 'ingewijden', maar breed uitgedragen wordt binnen de organisatie. Dit vraagt om een interne bewustwording hoe omgegaan moet worden met de belangen van personen die persoonsgegevens aan de gemeente Nieuwegein hebben toevertrouwd.

Om bewust te blijven van de risico's en de schade die kan ontstaan door gegevensbescherming niet serieus te nemen is een continue communicatie met betrekking tot dit onderwerp nodig. Binnen de kaders van de gemeente Nieuwegein wordt veel aandacht gegeven aan het bewustwordingsproces.

Er is gekozen om het thema informatieveiligheid en privacy zoveel mogelijk gezamenlijk op te pakken zodat er een logisch samenspel tussen deze twee thema's en het thema integriteit (dat veel lastiger te vatten is) bestaat. Zo zal voor deze drie thema's een gezamenlijk communicatieplan worden uitgewerkt en zal in de verdere communicatie gekeken worden hoe de thema's elkaar kunnen versterken. Voor de inbreng in het communicatieplan zorgen de CISO (informatieveiligheid) en de PO (privacy).

7.2 Bewustwording

Momenteel is binnen de gemeente Nieuwegein volop aandacht voor het thema privacy. Samen met de CISO en de PO (waar deze zijn aangewezen) werkt de kwartiermaker FG aan het compliant maken van de organisatie voor de AVG. In dat licht worden er ook bewustwordingsacties ontwikkeld. De bewustwordingsacties volgen de voortgang van het beleidsproces.

Voor een aantal verwerkingen van persoonsgegevens zullen de komende tijd PIA's worden uitgevoerd. De PIA zal de eerste periode worden begeleid vanuit de kwartiermaker FG en worden met medewerkers

van de teams ingevuld. Het doel om met medewerkers PIA's uit te voeren is tweeledig; betrokkenheid vergroten en het verzorgen van een leereffect, zodat sommige medewerkers later zelf een PIA kunnen uitvoeren.

Dit beleidsplan zal ook een bron vormen voor communicatie naar de afdelingen. Na vaststelling van het beleidsplan wordt het plan met de afdelingen besproken. Met de teammanagers zal vervolgens een lijn worden uitgedacht om jaarlijks activiteiten rond het thema 'privacy en informatieveiligheid' te bedenken met daarin aandacht voor bewustwording en gegevensbeveiliging.
Een belangrijk aandachtspunt hierbij is gebruik van email en internet. Hiervoor is een apart reglement opgesteld (zie bijlage 7).

7.3 Bewustwording door afdelingsactiviteiten

Uitgangspunt is om het bewustwordingsproces zo dicht mogelijk bij de medewerkers te organiseren. Welke communicatiemiddelen en trainingen worden ingezet ligt bij het afdelingsmanagement.

8 Beheer en opslag van persoonsgegevens

8.1 Opslag van persoonsgegevens

Persoonsgegevens worden binnen de gemeente Nieuwegein(vrijwel) altijd digitaal opgeslagen. Voor opslag van gegevens beschikken de gemeente Nieuwegein over een eigen, afgeschermd netwerk. De manier waarop gemeente Nieuwegeinhaar netwerk en gegevens beveiligen is in overeenstemming met de gemeentelijke beveiligingsnormen (BIG, zie ook 3.6)
Opslag gebeurt op de volgende manieren:

- In centrale databases die door verschillende gebruikers te benaderen en te bewerken zijn. Alle grote registraties van persoonsgegeven zijn in de gemeente Nieuwegein opgenomen in centrale databases.
- Binnen decentrale databases en spreadsheets die middels algemene kantoorautomatiseringssoftware te benaderen zijn. Dit betreft kleinschalige registraties met een zeer specifiek doel.
- Op ongestructureerde basis: in documenten, afbeeldingen en dergelijke. Dit betreft geen registraties maar specifieke persoonsgegevens over een of enkele personen.

Voor de opslag van persoonsgegevens gelden de volgende uitgangspunten:

- Opslag in centrale databases heeft sterk de voorkeur boven decentrale opslag. Centrale databases kennen een hogere beschikbaarheid, daarnaast is de integriteit en de vertrouwelijkheid van de data veel beter te waarborgen.
- Opslag van persoonsgegevens geschied op goed beveiligde netwerken waarover de gemeente Nieuwegein dienen te beschikken.
- Aan medewerkers die geregeld met persoonsgegevens op pad gaan zal een beveiligde voorziening worden aangeboden (smartphone, notebooks).
- Lokale opslag zoals smartphones en laptops worden afdoende versleuteld.

De gemeente Nieuwegein kent diverse voorzieningen om de beschikbaarheid van de persoonsgegevens te waarborgen. Vitale ICT-systemen en componenten zijn dubbel uitgevoerd, en alle gegevens op het interne netwerk worden dagelijks geback-upt. Ook deze maatregelen zijn in lijn met de gemeentelijke beveiligingsnormen.

8.2 Toegang tot en beheer van persoonsgegevens

Alleen geautoriseerde personen hebben toegang tot het netwerk van gemeente Nieuwegein en daarmee tot persoonsgegevens. Deze toegang tot het netwerk is beperkt tot applicaties en bestanden die vanuit de functie van de betrokkene noodzakelijk zijn. Voor toegang tot gestructureerde persoonsgegevens in centrale databases geldt een fijnmaziger toegang tot op specifiek gegevensniveau. Dit gebeurt op basis van rollen waarbij per medewerker of per functie een of meerdere rollen worden toegekend. Achter deze rollen hangt een autorisatieschema waarbij per type persoonsgegeven is vastgelegd in hoeverre deze vanuit de rol ingezien en veranderd mag worden. De toewijzing van rollen aan medewerkers wordt vastgelegd in autorisatiematrices en periodiek gecontroleerd.

De benodigde toegangsrechten worden vastgesteld door het afdelingsmanagement. Zij zijn verantwoordelijk voor de verwerking van persoonsgegevens (zie ook paragraaf 5.3) het beheer van de daarvoor benodigde applicaties en voor het treffen van afdoende beveiligingsmaatregelen. Het beheer van applicaties, en de daarin opgenomen persoonsgegevens en het daadwerkelijk toewijzen en inrichten van de toegangsrechten wordt uitgevoerd door applicatiebeheerders. De gemeente heeft hiervoor een formele procedure.

Toegang tot persoonsgegevens wordt op gegevens- en medewerkersniveau geregistreerd (gelogd). Op deze manier is te achterhalen wie op welk tijdstip welke gegevens heeft geraadpleegd. Gemeente Nieuwegein kent procedures om deze login te gebruiken bij privacy incidenten.

Bijlage 1 Overeenkomst verwerker/ gemeente Nieuwegein ex artikel 28 lid 3 AVG en/of artikel 7 Besluit basisregistratie personen

De verwerkersovereenkomst

Gemeente Nieuwegein, verder te noemen **Verwerkingsverantwoordelijke**, hierbij rechtsgeldig vertegenwoordigd door de <heer of mevrouw> <persoonsnaam>, <functie>
en
<Bedrijfsnaam>, gevestigd te <plaatsnaam>, verder te noemen **Verwerker**, hierbij rechtsgeldig vertegenwoordigd door de <heer of mevrouw> <persoonsnaam>, <functie>,

hierna afzonderlijk te noemen ''Partij", of gezamenlijk ''partijen"

Overwegen het volgende:
a) Partijen op <datum> de <titel hoofdovereenkomst>, hierna Hoofdovereenkomst, hebben afgesloten, op grond waarvan Verwerker de volgende dienst(en) levert aan de Verwerkingsverantwoordelijke: <specificatie dienst(en)>;
b) Verwerker verwerkt voor de uitvoering van de Hoofdovereenkomst Persoonsgegevens voor Verwerkingsverantwoordelijke;
c) Op de verwerking van Persoonsgegevens door Verwerker zijn de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet AVG van toepassing;
d) Partijen willen in aanvulling op de AVG en de Uitvoeringswet AVG de volgende afspraken over de verwerking van Persoonsgegevens vastleggen in deze Verwerkersovereenkomst.

Artikel 1 Definities
1.1 Begrippen uit de AVG en de Uitvoeringswet AVG die in deze Verwerkersovereenkomst worden gebruikt, hebben dezelfde betekenis.
1.2 Bijlagen: aanhangsels bij deze Verwerkersovereenkomst, die deel uitmaken van deze Verwerkersovereenkomst.

Artikel 2 Ingangsdatum en duur
2.1 Deze verwerkersovereenkomst gaat in op <datum> en duurt voort zolang de Verwerker als Verwerker van persoonsgegevens optreedt in het kader van de door de Verwerkingsverantwoordelijke ter beschikking gestelde persoonsgegevens voor < nader in te vullen omschreven doel>

Artikel 3 Onderwerp van deze verwerkersovereenkomst
3.1 Verwerker verwerkt de door via Verwerkingsverantwoordelijke ter beschikking gestelde persoonsgegevens uitsluitend in opdracht van Verwerkingsverantwoordelijke voor de uitvoering van de hoofdovereenkomst, behalve als wettelijke verplichtingen of bindende uitspraken van bevoegde organen anders bepalen.
3.2 De door Verwerker uit te voeren verwerkingen staan in bijlage < ... >, die Verwerker met behulp van Verwerkingsverantwoordelijke invult.

Artikel 4 Verplichtingen Verwerker
4.1 De Verwerker verwerkt gegevens ten behoeve van de Verwerkingsverantwoordelijke in overeenstemming met diens schriftelijke instructies.
4.2 Verwerker mag niet beslissen over de persoonsgegevens die hij heeft ontvangen voor de uitvoering van de hoofdovereenkomst. Zo neemt hij geen beslissingen o ver de ontvangst en het gebruik van deze gegevens, de verstrekking aan derden en de duur vande opslag van gegevens.
4.3 Als betrokkene een beroep doet op zijn rechten, zoals inzage, correctie of verwijdering, helpt Verwerker Verantwoordelijke om daarop binnen de wettelijke termijnen een beslissing te nemen.
4.4 Als Verwerkingsverantwoordelijke een gegevensbeschermingseffectbeoordeling of een audit wil uitvoeren en de hulp van Verwerker daarbij nodig heeft, dan maken partijen daarover afspraken.

Artikel 5 Geheimhoudingsplicht

5.1 De Verwerker is verplicht tot geheimhouding van documenten en persoonsgegevens, waarvan zij bij het verwerken ten behoeve van de Verwerkingsverantwoordelijke ter uitvoering van de dienstverleningsovereenkomst kennisneemt en zal deze plicht ook aande bij haar in dienst zijnde dan wel de door haar ingezette personen, instanties en subverwerkers opleggen. Na beëindiging van deze verwerkersovereenkomst zal de geheimhoudingsplicht uit hoofde van dit artikel blijven bestaan.

5.2 Indien de Verwerker op grond van een wettelijke verplichting gegevens dient te verstrekken, zal de Verwerker de grondslag van het verzoek en de identiteit van de verzoeker verifiëren en zal de Verwerker de Verwerkingsverantwoordelijke onmiddellijk, voorafgaand aan de verstrekking ter zake informeren, tenzij wettelijke bepalingen dit verbieden.

Artikel 6 Meldplicht datalekken en beveiligingsincidenten

6.1 Verwerker zal de Verwerkingsverantwoordelijke onverwijld – doch uiterlijk binnen 24 uur na de eerste ontdekking – informeren over alle (vermoedelijke) 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 in geval van niet-nakoming.

6.2 De Verwerker beschikt over een gedegen plan van aanpak betreffende de omgang met en afhandeling van inbreuken en zal de Verwerkingsverantwoordelijke, op diens verzoek, inzage verschaffen in het plan. Verwerker stelt de Verwerkingsverantwoordelijke op de hoogte van materiele wijzigingen in het plan van aanpak.

6.3 Verwerker zal het doen van meldingen aan de toezichthouders(s) overlaten aan de Verwerkingsverantwoordelijke.

6.4 Verwerker 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).

6.5 Verwerker houdt een gedetailleerd logboek bij van alle (vermoedens van) in breuken op de beveiliging, evenals de maatregelen die in vervolg op dergelijke inbreuken zijn genomen en geeft daar op eerste verzoek van de Verwerkingsverantwoordelijke inzage in.

Artikel 7 Beveiligingsmaatregelen en controle

7.1 Verwerker neemt alle passende technische en organisatorische maatregelen om de persoonsgegevens welke worden verwerkt ten dienste van de Verwerkingsverantwoordelijke te beveiligen en beveiligd te houden tegen verlies of ten enige vorm van onrechtmatige verwerking conform bijlage 3.

7.2 Verwerkingsverantwoordelijke is te allen tijde gerechtigd de verwerking van persoonsgegevens te (doen) controleren. Verwerker is verplicht de Verwerkingsverantwoordelijke of de door Verwerkingsverantwoordelijke ingeschakelde externe controleur toe te laten en verplicht medewerking te verlenen zodatde controle daadwerkelijk uitgevoerd kan worden.

7.3 Verwerkingsverantwoordelijke zal de controle slechts (laten) uitvoeren na een voorafgaande schriftelijke melding aan Verwerker.

7.4 Verwerker verbindt zich om binnen een door de Verwerkingsverantwoordelijke te bepalen termijn de Verwerkingsverantwoordelijke of de externe controleur te voorzien vande verlangde informatie. Hierdoor kan de Verwerkingsverantwoordelijke of de externe controleur zich een gedegen oordeel vormen over de naleving door de Verwerker van deze Verwerkersovereenkomst. De Verwerkingsverantwoordelijke of de externe controleur is gehouden alle informatie betreffende deze controles vertrouwelijk te behandelen.

7.5 Verwerker staat er voor in, de door de Verwerkingsverantwoordelijke of de externe controleur aangegeven aanbevelingen ter verbetering binnen de daartoe door de Verwerkingsverantwoordelijke te bepalen redelijke termijn uit te voeren.

7.6 De redelijke kosten van de controle worden gedragen door de partij die de opdracht geeft, tenzij uit de controle blijkt dat de Verwerker enig punt uit deze Verwerkersovereenkomst niet heeft nageleefd. In dat geval worden de kosten van de controle gedragen door de Verwerker.

7.7 Verwerker rapporteert, op verzoek en maximaal éénkeer per jaar, over de opzet en werking van het stelsel van maatregelen en procedures, gericht op naleving van deze Verwerkersovereenkomst.

7.8 Naast de hierboven bedoelde controles en rapportages kunnen partijen overeenkomen gebruik te maken van een Third Party Memorandum (TPM) opgesteld door een onafhankelijke externe deskundige.

Artikel 8 Inschakeling derden

8.1 De Verwerker is slecht gerechtigd de uitvoering van de werkzaamheden geheel of ten dele uit te besteden aan derden na voorafgaande, duidelijk gespecificeerde, schriftelijke toestemming van de Verwerkingsverantwoordelijke.
8.2 De Verwerkingsverantwoordelijke kanaan de schriftelijke toestemming voorwaarden verbinden, op het gebied van geheimhouding en ter naleving van de verplichtingen uit deze verwerkersovereenkomst.
8.3 De Verwerker blijft in deze gevallen te allen tijde aanspreekpunten verantwoordelijk voor de naleving van de bepalingen uit deze verwerkersovereenkomst. De Verwerker garandeert dat deze derden schriftelijk minimaal dezelfde plichten op zich nemen als tussen de Verwerkingsverantwoordelijke en de Verwerker zijn overeengekomen en zal de Verwerkingsverantwoordelijke, op diens verzoek, inzage verschaffen in de overeenkomsten met deze derden waarin deze plichten zijn opgenomen.
8.4 De Verwerker mag de persoonsgegevens uitsluitend verwerken in Nederland dan wel binnen de EU. Doorgifte naar derde landen is uitsluitend toegestaan na voorafgaande schriftelijke toestemming van de Verwerkingsverantwoordelijke en met inachtneming van de toepasselijke wet- en regelgeving.
8.5 De Verwerker houdt een actueel register bij van de door hem ingeschakelde derden en onderaannemers waarin de identiteit, vestigingsplaats en een beschrijving van de werkzaamheden van de derden of onderaannemers zijn opgenomen, alsmede eventuele door de Verwerkingsverantwoordelijke gestelde aanvullende voorwaarden. Dit register zal als bijlage <...>aan deze verwerkersovereenkomst worden toegevoegd en zal door de Verwerker actueel worden gehouden.

Artikel 9 Wijzigen en beëindigen verwerkersovereenkomst

9.1 Wijzigen van deze verwerkersovereenkomst kan slecht schriftelijk plaatsvinden middels eendoor beide partijen geaccordeerd voorstel.
9.2 Verwekingsverantwoordelijke en Verwerker treden met elkaar inoverleg over wijzigingen indeze verwerkersovereenkomst als wijziging in regelgeving of eenwijziging in de uitleg van regelgeving daartoe aanleiding geven.
9.3 Na afloop van de werkzaamheden, zal Verwerker op verzoek van Verwerkingsverantwoordelijke de ter beschikking gestelde Persoonsgegevens aan Verwerkingsverantwoordelijke teruggeven en/of vernietigen.
9.4 Verwerkingsverantwoordelijke kan nadere redelijke eisen stellen aan de wijze van beschikbaarstelling, waaronder eisen aan het bestandsformaat, dan wel vernietiging. Deze werkzaamheden moeten, binnen een nader overeen te komen redelijke termijn, uitgevoerd worden.
9.5 Verwerker maakt hiervan een verslag en geeft dit aan Verwerkingsverantwoordelijke.

Artikel 10 Aansprakelijkheid

10.1 Als verwerker toerekenbaar tekortkomt in de nakoming van zijn verplichting(en), is verwerker tegenover verwerkersverantwoordelijke, alsmede zijn personeel en door verwerkersverantwoordelijke ingeschakelde derden, aansprakelijk voor de vergoeding van alle geleden en/of te lijden schade. Deze aansprakelijkheid is, behoudens aanspraken als gevolg van schadevergoeding ten gevolge van dood of letsel en/of opzet- of grove schuld aan de zijde van verwerkersverantwoordelijke en/of diens personeel en/of in geval van schending van intellectuele eigendomsrechten, beperkt tot eenbedrag van € 1.000.000,- per gebeurtenis met een maximum van € 2.500.000,-.per jaar.
102. Onder een niet-toerekenbare tekortkoming (overmacht) wordt in ieder geval niet verstaan: gebrek aan personeel, stakingen, ziekte van personeel, tekort aan dan wel verlate aanlevering of ongeschiktheid van voor het verrichten van de Prestatie benodigde programmatuur, materialen, transportproblemen, storingen, enig tekortschieten van ingeschakelde derden. Voorts wordt niet onder niet/toerek enbare tekortkoming begrepen wanprestatie van door de tekortkomende Partij ingeschakelde derden en/of liquiditeits/ c.q. solvabiliteitsproblemen van de tekortkomende Partij of door hem ingeschakelde derden.

Artikel 11 Toepasselijk recht

11.1 Op deze verwerkersovereenkomst enop alle geschillen die daaruit mogen voortvloeien of daarmee mogen samenhangen, is in het Nederlands recht van toepassing.

Artikel 12 Overige bepalingen

12.1 Alle geschillen, ook als alleen één partij vindt dat er een geschil is, zu llen in eerste instantie worden voorgelegd aan de bevoegde rechter van de Rechtbank Midden- Nederland.
122. Alle rechten en verplichtingen uit de hoofdovereenkomst, waaronder begrepen de van toepassing zijnde algemene voorwaarden, zijn voor het overige aanvullen d van toepassing op de verwerking van persoonsgegevens.

Ondertekening

Aldus overeengekomen en in tweevoud ondertekend,

Gemeente Nieuwegein <Naam organisatie>
namens deze: <naam, functie> namens deze <naam, functie>

plaats <.....> plaats <.....>
datum <.....> datum <.....>

Overzicht van te verwerken persoonsgegevens

1. Naam verwerking, doeleinden, categorieën van betrokkenen, (bijzondere) persoonsgegevens en eventuele doorgifte naar derde landen.

Naam verwerking	**Verwerkings - doeleinden**	**Categorieën van Betrokkenen**	**(Bijzondere) Persoonsgegevens**	**Doorgifte naar derde landen**

2. Contactgegevens

Contactpersoon Verwerkingsverantwoordelijke (NB: Ook buiten kantooruren)	Naam: Contactgegevens:
Contactpersoon Verwerker (NB: Ook buitenkantooruren)	Naam: Contactgegevens:

3. Ingeschakelde subverwerkers

Naam en contactgegevens subverwerker	**uitbestede verwerkingen**

N B : Eventuele wijzigingen in bovenstaande tabellen geven partijen op korte termijn aan elkaar door.

Inlichtingen om datalekken en andere incidenten te beoordelen

Stap 1
Verwerker zal alle (voor zover haar bekend) inlichtingen verschaffen d ie Verwerkingsverantwoordelijke noodzakelijk acht om het incident te kunnen beoordelen.

Daarbij verschaft Verwerker de volgende informatie aan Verwerkingsverantwoordelijke:
- wat de (vermeende) oorzaak is van de inbreuk;
- wat het (vooralsnog bekende en/of te verwachten) gevolg is;
- wat de (voorgestelde) oplossing is;
- contactgegevens voor de opvolging van de melding;
- aantal personen waarvan gegevens betrokken zijn bij de inbreuk (indien geen exact aantal bekend is: het minimale en maximale aantal personen waarvan gegevens betrokken zijn bij de inbreuk);
- een omschrijving van de groep personen van wie gegevens betrokken zijn bij de inbreuk;

- het soort of de soorten persoonsgegevens die betrokken zijn bij de inbreuk;
- de datum waarop de inbreuk heeft plaatsgevonden (indien geen exacte datum bekend is: de periode waarbinnen de inbreuk heeft plaatsgevonden);
- de datum en het tijdstip waarop de inbreuk bekend is geworden bij Verwerker of bij eendoor hem ingeschakelde derde of onderaannemer;
- of de gegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk zijn gemaakt voor onbevoegden;
- wat de reeds ondernomen maatregelen zijn om de inbreuk te beëindigen en om de gevolgen van de inbreuk te beperken.

Stap 2
Verwerker houdt een gedetailleerd logboek bij:
- van alle vermoedens van inbreuken op de beveiliging;
- van alle inbreuken op de beveiliging;
- de maatregelen die in vervolg op dergelijke inbreuken zijn genomen.

Verwerker geeft op eerste verzoek van de Verwerkingsverantwoordelijke inzage in het logboek.

Aantonen passend niveau van beveiliging
1. Normenstelsel
□ De informatiebeveiliging vindt plaats volgens algemeen erkende normen, namelijk:
……
……..(vermeld normenstelsel, zoals bijvoorbeeld NEN7510, NEN/ISO 27001, PCI/DSS).

□ De informatiebeveiliging vindt plaats volgens een algemeen erkende overheidsnorm zoals de BIG (of de BIR, BIO) of vergelijkbaar, namelijk:
……..

2. De toereikendheid van de informatiebeveiliging blijkt uit:
□ Periodieke externe controles zoals audits of TPM's (bijv. ISAE3xxx SOC type II);
□ Een Assurance rapport van een auditor die is aangesloten bij NOREA;
□ Data Pro Certificaat
□ Eigen controles of eigen mededelingen over de beveiligingsmaatregelen zoals hieronder beschreven:
……

Uit de certificering/periodieke externe controles/audits of uit de eigen controles/beschrijvingen blijkt of kan afgeleid worden dat de beveiliging passend is bij de verwerking(en) genoemd in bijlage 1.

Bijlage 2 Protocol gegevensverstrekking aan andere verwerkingsverantwoordelijken

Voor de uitvoering van taken kan de gemeente voor verwerking van persoonsgegevens samenwerking aan gaan met andere verwerkingsverantwoordelijken. Binnen de samenwerkingsrelatie blijven alle betrokken verwerkingsverantwoordelijken zelfstandig verantwoordelijk voor de 'eigen' verwerkingen.

Dit protocol voorziet in de werkwijze bij de verstrekking van persoonsgegevens door de gemeente aan de samenwerkingsrelatie om een gezamenlijk doel te bereiken voor zover deze persoonsgegevens noodzakelijk zijn voor de uitvoering van de taken van de desbetreffende samenwerkingsverband. Met inachtneming van het bij of krachtens de Algemene Verordening Gegevensbescherming (AVG) bepaalde geschiedt het verstrekken van persoonsgegevens overeenkomstig dit protocol.

Dit protocol gegevensverstrekking is geldend vanaf ..... en wordt voorafgaande aan elke eerste verstrekking voor een bepaald doel aan de partners in het samenwerkingsverband gezonden.

Protocol

1. In gevallen waarin de samenwerkingspartner(s) persoonsgegevens willen ontvangen van de gemeente ter uitoefening van hun taken in de samenwerkingsafspraken, dien(t)en zij een daartoe strekkend verzoek in bij de desbetreffende gemeente. In het verzoek worden de volgende onderwerpen beschreven:
   - Doel en grondslag van de verwerking,
   - Aantonen of contractspartij verwerkingsverantwoordelijke is,
   - Welke persoonsgegevens men van de gemeente wenst te ontvangen,
   - Welke passende technische en organisatorische maatregelen de contractspartij heeft genomen om persoonsgegevens te verwerken,
   - Welke maatregelen zijn genomen om verdere onrechtmatige verwerking te voorkomen,
   - Vanaf welke datum overdracht van persoonsgegevens zal geschieden.

2. Voor de uitvoering van wettelijke taken door de samenwerkingspartner kan de gemeente alle bij haar bekende persoonsgegevens in een concrete situatie of in een verzameling concrete situaties ter verwerking overdragen aan de ander onder de restrictie dat enkel die persoonsgegevens worden overgedragen waarbij de samenwerkingspartner een aanwijsbaar belang heeft ten behoeve van de uitvoering van diens wettelijke taken.

3. Indien door de contractspartner geen wettelijke taak wordt uitgevoerd kan de gemeente alle bij haar bekende persoonsgegevens in een concrete situatie ter verwerking overdragen aan de samenwerkingspartner, indien noodzakelijk ter bescherming van een vitaal belang van de betrokkene of diens naasten onder de restrictie dat enkel die persoonsgegevens worden overgedragen waarbij de samenwerkingspartner een aanwijsbaar belang heeft ten behoeve van de uitvoering van diens werkzaamheden. Indien de wettelijke grondslag en het vitaal belang ontbreken is overdracht van persoonsgegevens enkel mogelijk met uitdrukkelijke toestemming van de betrokkene.

4. De persoonsgegevens die op grond van artikel 2 en 3 van de gemeente worden ontvangen zullen door de contractspartners worden verwerkt met inachtneming van de wettelijke voorschriften, waaronder de AVG, in welk kader de samenwerkingspartners voorafgaand aan de eerste verstrekking een privacy beleid zullen opstellen dat in overeenstemming is met dit protocol. Een exemplaar van dit beleidsplan zal aan de gemeente ter hand worden gesteld.

5. Voor de uitvoering van de verwerking door de contractspartners die geen verwerkingsverantwoordelijke zijn zal tussen gemeente en de contractspartner een overeenkomst als bedoeld in artikel 28 lid 3 AVG en/of artikel 7 Besluit basisregistratie personen worden opgesteld.

6. Contractspartners zullen de gemeente onmiddellijk op de hoogte stellen van een datalek als bedoeld in artikel 33 AVG, alle noodzakelijke maatregelen nemen om het lekken te doen stoppen en om alle informatie en medewerking te verlenen waar de gemeente om verzoekt.

7. Samenwerkingspartners zullen de van de gemeente verkregen persoonsgegevens niet verder verwerken op een wijze die onverenigbaar is met de doeleinden waarvoor de persoonsgegevens zijn verkregen. Samenwerkingspartners zullen de persoonsgegevens niet openbaren of aan derden verstrekken, behoudens voor zover daartoe een wettelijke verplichting bestaat. Verdere verwerking van de persoonsgegevens voor statistische of wetenschappelijk doeleinden wordt niet als onverenigbaar beschouwd, indien de nodige voorzieningen zijn getroffen ten einde te verzekeren dat de verdere verwerking uitsluitend geschiedt ten behoeve van deze specifieke doeleinden.

8. Overdracht van de aansprakelijkheid voor onrechtmatige verwerkingen geschiedt op het moment dat de gemeente voor de eerste maal persoonsgegevens overdraagt aan de samenwerkingspartner.

Bijlage 3 Geheimhoudingsverklaring inhuur derden

Geheimhoudingsverklaring inhuur derden

Ondergetekende inhuurmedewerker (hierna te noemen medewerker) verklaart zich te houden aan de volgende bepalingen:

Artikel 1 Verplichtingen inzake geheimhouding

1.1 De medewerker zal alle informatie, met uitzondering van informatie waarvan uit een algemeen toegankelijke bron kennis kan worden genomen, over de gemeente of de activiteiten of producten van de gemeente waaronder maar niet uitsluitend strategie, meerjaren- en operationele plannen, informatie van technologische aard, calculaties, prijsstellingen, omzet, marges, knowhow, productspecificaties, computerprogramma's en methodieken, met inbegrip van informatie over cliënten, leveranciers, gemeentes en andere relaties, en al zulke informatie over maatschappijen die behoren tot de organisatie waarvan de gemeente deel uitmaakt, niet gebruiken of aan enige derde openbaren, behalve voor zover dat voor de uitoefening van de werkzaamheden van medewerker noodzakelijk is. De medewerker zal zulke informatie zorgvuldig bewaren en ervoor zorgen dat een derde daarvan niet anders dan in overeenstemming met dit lid kennis krijgt.

1.2 Lid 1 van dit artikel geldt niet voor zover de medewerker tot gebruik of openbaarmaking verplicht is op grond van de wet of een uitspraak van de rechter of een ander bevoegd overheidsorgaan.

1.3 De medewerker moet alle zaken van de gemeente, daaronder begrepen (digitale) documenten, computer(diskettes) en andere (digitale) informatiedragers, met inbegrip van kopieën daarvan, die de medewerker in verband met de uitoefening van diens werkzaamheden onder zich krijgt, niet anders gebruiken en niet langer onder zich houden dan voor de uitoefening van diens werkzaamheden noodzakelijk is en in ieder geval terstond aan de gemeente (terug)geven indien de gemeente dat verlangt of, eigener beweging, indien de medewerker diens werkzaamheden tijdelijk of blijvend niet uitoefent of de werkopdracht is geëindigd.

1.4 Voor zover informatie als bedoeld in lid 1 is opgeslagen in een computersysteem van de medewerker of anderszins is vastgesteld in een vorm die de medewerker niet op grond van lid 3 aan de gemeente behoeft (terug) te geven, zal de medewerker die informatie niet langer bewaren dan voor de uitoefening van de werkzaamheden van de medewerker noodzakelijk is en in ieder geval terstond vernietigen indien de gemeente dat verlangt of, eigener beweging, indien de medewerker diens werkzaamheden om welke reden dan ook tijdelijk of blijvend niet uitoefent of de werkopdracht is geëindigd.

Artikel 2 Toegang tot gebouwen en apparatuur

2.1 De medewerker gebruikt de hulpmiddelen voor toegang tot locaties, apparatuur en ruimten van de gemeente uitsluitend voor het doel waarvoor deze aan de medewerker ter beschikking zijn gesteld. De medewerker probeert niet om onbevoegd toegang te krijgen tot locaties van de gemeente. Voor de medewerker bestemde toegangsmiddelen behoudt deze voor zichzelf en geeft deze niet aan collega's of derden, tenzij daarover afspraken zijn gemaakt met de gemeente en dit past in de bedrijfsvoering.

2.2 Bij vermissing, ontvreemding, misbruik of ander onrechtmatig gebruik van de aan de medewerker verstrekte toegangspas, sleutels, tags, toegangscodes, apparatuur of software stelt de medewerker de daartoe aangewezen personen binnen het organisatieonderdeel waar deze werkzaam is onmiddellijk daarvan in kennis.

2.3 De medewerker houdt zich aan de regels die per locatie van de gemeente zijn gesteld ten aanzien van het ontvangen en begeleiden van bezoekers.

Artikel 3 Omgang met informatie

3.1 De medewerker laat geen stukken onbeheerd achter, ook niet op diens bureau, in de ruimte of (thuis)werkplek waar de medewerker werkt, waarvan de medewerker weet of zou kunnen weten dat deze vertrouwelijk zijn. De medewerker houdt zich op diens (thuis)werkplek aan de regels voor de beveiliging van informatie. Als de medewerker vermoedt dat er een inbreuk wordt gemaakt op de informatieveiligheid dan doet de medewerker daarvan een melding aan de gemeente.

3.2 Documenten, e-mails, en overige zaken die niet voor de medewerker bestemd zijn, zendt de medewerker onmiddellijk door aan het juiste adres of retourneert deze aan de afzender. Is het juiste adres noch de afzender bekend, dan vernietigt de medewerker ze.

Artikel 4 Omgang met bedrijfsmiddelen

4.1 De medewerker gaat zorgvuldig om met alle aan de medewerker ter beschikking gestelde bedrijfsmiddelen, zowel op diens werkplek als elders waar de medewerker bedrijfsmiddelen gebruikt. De medewerker houdt zich aan de geldende regels voor internet en e-mail gebruik en de huisregels van de organisatie. De medewerker laat geen waardevolle bedrijfsmiddelen onbeheerd achter op diens werkplek of elders waar de medewerker bedrijfsmiddelen gebruikt.

Artikel 5 Integriteit

5.1 De medewerker gedraagt zich integer, wat in ieder geval inhoudt dat de medewerker zich houdt aan de interne regels over integriteit en de huisregels van de organisatie.

5.2 Als de medewerker een misstand constateert, meldt de medewerker deze in eerste bij de gemeente of diens superieur. Als de medewerker anoniem wil blijven, zal deze gebruik maken van de Klokkenluiderregeling en meldt een geconstateerde misstand bij de vertrouwenspersoon integriteit.

5.2 Bij twijfel raadpleegt de medewerker de vertrouwenspersoon integriteit.

Artikel 6 Omgangsvormen

6.1 De medewerker houdt zich aan correcte omgangsvormen en houdt zich aan de interne regels over ongewenst gedrag, omgangsvormen en de huisregels van de organisatie.

6.2 Krijgt de medewerker te maken met ongewenste omgangsvormen dan kan deze de gemeente raadplegen, dan wel de vertrouwenspersoon. Wordt het probleem niet opgelost dan kan de medewerker een klacht indienen bij de klachtencommissie van de organisatie.

Artikel 7 Duur van de verplichtingen

7.1 Na de beëindiging van de opdracht/overeenkomst blijven de uit deze verklaring voortvloeiende verplichtingen bestaan zolang de informatie genoemd in artikel 1, lid 1 niet:

a) publiekelijk bekend is of deel uit maakt van de publiekelijk toegankelijke literatuur zonder schending van enige geheimhoudingsplicht door de medewerker;

b) door enige derde (anders dan enige persoon handelend namens de gemeente aan de medewerker bekend is gemaakt en deze derde vrijelijk over genoemde informatie mocht beschikken zonder enige geheimhoudingsverplichting.

Naam medewerker Handtekening:

Functie

Datum

Plaats

Bijlage 4 Privacystatement

https://www.nieuwegein.nl/privacystatement/

Bijlage 5 Protocol procedure melden datalekken

In deze procedure maken we duidelijk hoe je een datalek moet melden. In dat stappenplan wordt ook verwezen naar de definities van de begrippen ‘datalek’ en ‘persoonsgegevens’.

Daarnaast willen we graag benadrukken hoe belangrijk en ook welkom het is dat medewerkers datalekken melden. Van elk datalek kunnen we als organisatie leren.

A. Melden van een (potentieel) datalek

Stap 1: Beoordeel of het een datalek is. Dit kun je doen aan de hand van de tekst en het stroomschema op de volgende pagina’s. Indien je twijfelt, behandel de situatie dan als een datalek en ga verder met stap 2.
Stap 2: Stuur een e-mail naar Privacy Officer. Zet je (team) manager altijd in de ‘Cc:’.

Wat zet je in de e-mail?

- *Wie* zijn er betrokken? (Denk hierbij aan inwoner, zorgaanbieder enz. Het noemen van de naam of andere persoonsgegevens van de betrokkene is niet nodig.)
- *Wat* is er precies gebeurd? (Denk hierbij aan versturen e-mail naar verkeerde persoon.)
- *Welke* soorten persoonsgegevens zijn hierbij aan de orde? (Denk hierbij aan NAW, BSN, etc.)
- *Waar* is het gebeurd? (Denk hierbij aan in trein, op straat.)
- *Hoe* is het gebeurd? (Denk hierbij aan verlies pc of dossier.)
- *Waarom* is het gebeurd? (Denk hierbij aan versturen zorgdossier naar zorgaanbieder.)
- *Wanneer* is het gebeurd? (Denk hierbij aan datum en tijdstip.)
- Welke *directe actie* heb je al ondernomen? (Denk hierbij aan proberen datalek te herstellen zoals het terugroepen van de e-mail.)
- Indien het mogelijk is, stuur je een kopie van de data met de e-mail mee. Als je bijvoorbeeld een mail naar de verkeerde persoon hebt gestuurd, voeg je een kopie van de betreffende mail toe aan de mail naar de Privacy Officer.

Hoe completer jouw mail naar de Privacy Officer, des te sneller er gehandeld kan worden.
Stap 3: De Privacy Officer onderzoekt wat er verder moet gebeuren. Hij zal contact met jou opnemen om eventuele vervolgstappen te bespreken.

Als medewerker ben je bij stap 1 en stap 2 aan zet. Na stap 2 zal de Privacy Officer, indien van toepassing, melding doen bij de Autoriteit Persoonsgegevens. Hij mailt jou en je team manager een concept van de te maken melding bij de AP ter controle van de juistheid en volledigheid. Daarnaast zal hij aan jou aangeven of de betrokkene(n) geïnformeerd moet(en) worden, dit is namelijk niet altijd het geval.

B. Wat is een datalek?

Bij een datalek denken de meeste mensen vooral aan hacken. Logisch ook, want dat zijn de datalekken die in het nieuws komen. Datalekken vinden echter regelmatig plaats. Vaak worden ze niet eens opgemerkt of geregistreerd, omdat het bedrijf waar het datalek plaatsvond het incident niet als zodanig herkent. Dat is problematisch, want de wet stelt nogal wat eisen op het gebied van datalekken. De term ‘datalek’ komt niet voor in de wet. De Algemene Verordening Gegevensbescherming (AVG) heeft het in plaats daarvan over een ‘inbreuk in verband met persoonsgegevens’. De AVG definieert dit als volgt: *‘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.’.*
In normaal Nederlands wil dat zeggen dat er sprake is van vernietiging, verlies, wijziging of delen van persoonsgegevens zonder dat dit de bedoeling was.
C. Wat zijn persoonsgegevens?

Persoonsgegevens zijn volgens de AVG

> *‘Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon; als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.’.*

Voorbeelden van persoonsgegevens zijn:

- Naam
- Adres
- Geboortedatum
- Geboorteplaats
- IP-adres
- BSN-nummer
- Klantnummers bij bedrijven
- E-mailadres
- Uiterlijke kenmerken
- Medische informatie
- Informatie over inkomen
- Informatie over hobby's
- Online zoekgeschiedenis
- Telefoonnummer
- Kenteken
- IMEI-nummer van een telefoon
- Filmopnames
- Geluidsopnames
- Foto's
- Personeelsdossier
- IBAN
- Wachtwoorden
- Locatiegegevens
- Etc.

Sommige van deze gegevens zijn zogenaamde bijzondere persoonsgegevens. Bijzondere persoonsgegevens zijn gegevens van een gevoelige aard. Het zijn gegevens die op juridische gronden of om ethische redenen extra bescherming nodig hebben. Op basis van deze gegevens kan iemand bijvoorbeeld worden gediscrimineerd. Dit zijn allemaal bijzondere persoonsgegevens:

- Ras of etnische afkomst;
- Politieke opvattingen;
- Religie of levensbeschouwing;
- Lidmaatschap van een vakbond;
- Genetische gegevens;
- Biometrische gegevens;
- Gegevens over gezondheid;
- Geaardheid of gegevens over iemands seksueel gedrag.

Een datalek hoeft niet per se opzettelijk te zijn, zoals bij hacking. Er kan ook sprake zijn van onopzettelijke datalekken, bijvoorbeeld als persoonsgegevens per abuis worden gedeeld met de verkeerde persoon. Het hoeft daarbij niet te gaan om persoonsgegevens van duizenden mensen, een datalek kan ook betrekking hebben op slechts één persoon. Sterker nog, in bijna de helft van de datalekken in het derde kwartaal van 2017 was er sprake van een datalek met betrekking tot één persoon en ruim de helft van het aantal datalekken betreft het e-mailen naar een verkeerd e-mailadres.

Kort gezegd zijn er dus drie soorten datalekken. Persoonsgegevens zijn opzettelijk of per ongeluk:
- openbaar of toegankelijk gemaakt (inbreuk op vertrouwelijkheid);
- niet toegankelijk of vernietigd (inbreuk op beschikbaarheid);
- gewijzigd (inbreuk op integriteit).

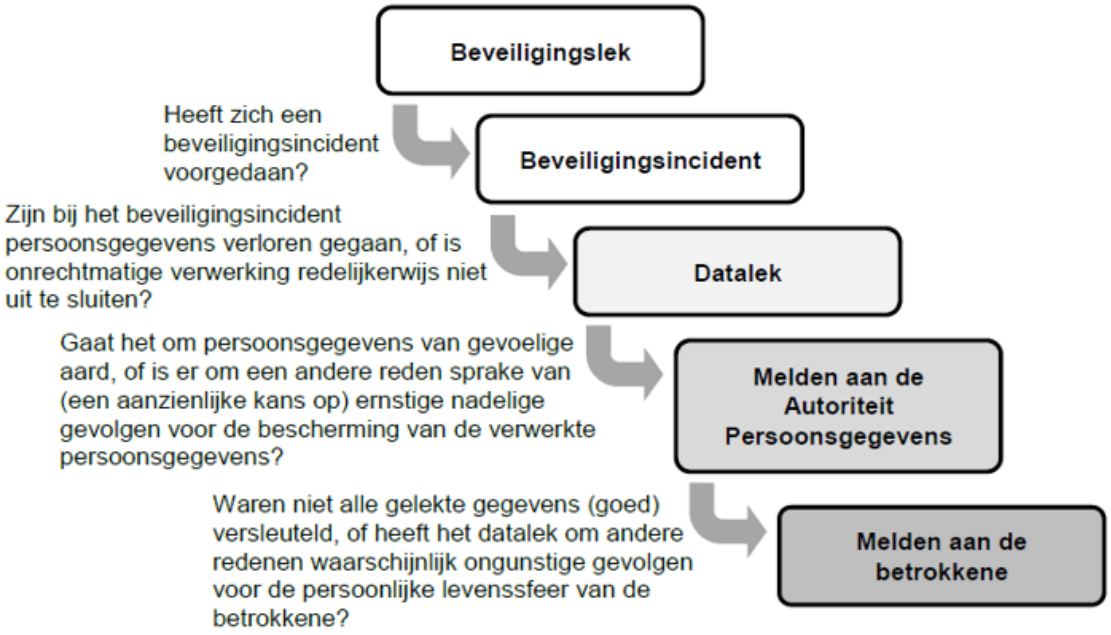
Een datalek kan overigens onder meerdere categorieën vallen; de ene categorie sluit de andere namelijk niet uit.
- Voorbeelden van datalekken

Je hebt hierboven kunnen lezen wat een datalek inhoudt, maar hoe ziet dat uit in de praktijk? Hieronder volgen een aantal voorbeelden.
- Brief of pakketje of e-mail naar verkeerde ontvanger
- Persoonsgegevens delen met verkeerde ontvanger of collega
- Dossier in trein laten liggen
- Persoonsgegevens bij het oud papier

- Persoonsgegevens op oud apparaat (nieuwe laptop, smartphone of welk ander apparaat dan ook)
- Apparaat met persoonsgegevens kwijtraken
- Een onherstelbaar defect apparaat (zonder back-up)
- Sleutel voor versleutelde gegevens is verloren of vergeten
- Toegang door ongeautoriseerde partij

Welke stappen doorlopen we bij het bepalen van een datalek?

De Autoriteit Persoonsgegevens heeft een handig schema om te bepalen wanneer er sprake is van een datalek en hoe ernstig het is:



Bijlage 6 Protocol integrale gegevensverwerking in het sociale domein gemeente Nieuwegein: Jeugdwet, Wmo 2015, Wet gemeentelijke schuldhulpverlening, Participatiewet

Inleiding

In het kader van integrale hulpverlening binnen het sociaal domein bestaat bij verschillende netwerkpartners van de gemeente zoals WIL, welzijnsorganisaties, GGDrU (Jeugdgezondheidszorg en het Meldpunt Zorg en Overlast), artsen, verpleegkundigen en hulpenwoningcorporaties, politie, justitie, GGZ, behoefte aan het uitwisselen van persoonsgegevens om elkaar te informeren in geval van het bieden van passende hulp aan inwoners.
Binnen elk wettelijk kader gelden afzonderlijke regels met betrekking tot verwerking van persoonsgegevens. Er is geen overkoepelende wet die gemeenten bevoegdheden geeft de gegevensverwerking tussen de verschillende instanties/netwerkpartners regelt. Dit protocol bevat een concrete handleiding voor integrale gegevensverwerking in het sociaal domein.

Integrale gegevensverwerking

Onder integrale gegevensverwerking wordt verstaan: de verwerking van persoonsgegevens dwars door de verschillende sectoren van het sociale domein heen.

Toestemming

De ondubbelzinnige toestemming van de betrokken inwoner is de basis voor integrale gegevensverwerking. Ondubbelzinnige toestemming betekent dat de toestemming op basis van voldoende informatie, in vrijheid wordt gegeven. Als er geen ruimte is om nee te zeggen (ook ten aanzien van het formulier voor het aanvragen van hulp) dan is er geen sprake van ondubbelzinnige toestemming.
Het vragen van een algemene toestemming voor gegevensverwerking is dan ook niet toegestaan. De gegevensverwerking waar toestemming voor gevraagd zal altijd concreet gemotiveerd en telkens gedocumenteerd moeten worden in het dossier van de betrokkene.

Conflict van plichten/ vitaal belang

Alleen in geval van conflict van plichten of een vitaal belang kan afgeweken worden van de toestemmingseis.

Stappenplan integrale gegevensverwerking

Dit stappenplan is een hulpmiddel bij vragen omtrent een zorgvuldige uitwisseling van informatie in verband met het bieden van integrale hulp en ondersteuning (integrale gegevensverwerking).

Stap 1 Bepaal op basis van de hulpvraag of integrale gegevensverwerking noodzakelijk is
De hulpvraag is leidend bij het vaststellen welke informatie nodig is. In een gesprek met de inwoner wordt de vraag verhelderd om te kijken of er wellicht 'een vraag achter de vraag' tevoorschijn komt. Is de hulpvraag verhelderd, dan kan worden vastgesteld welke informatie nodig is om antwoord te geven op de hulpvraag. Leidend hierbij is de bepaling in de AVG dat niet meer gegevens mogen worden verwerkt dan noodzakelijk is voor het doel. In veel gevallen zal het ook na vraagverheldering blijken te gaan om een hulpvraag waarvoor gegevensverwerking binnen één domein voldoende is.

Deze stap vraagt van de gemeente of het lokale team om kritisch te beoordelen of het welnoodzakelijk is om breed te inventariseren ofte overleggen. Zijn daar geen aanwijzingen voor, dan wordt de hulpvraag 'gewoon' afgehandeld volgens de regels van het betreffende domein. Zijn daar wel aanwijzingen voor dan worden de vervolgstappen gezet (ook als die aanwijzingen pas tijdens het traject naar voren komen).

Stap 2 Bepaal het doel van het overleg of van de integrale gegevensverwerking
Uit Stap 1 kan volgen dat informatie nodig is uit andere domeinen of dat overleg in het gehele wijkteam nodig is. Dan is het van belang om vast te stellen, welke informatie er nodig is en welk doel met de informatie moet worden bereikt.

Soms zal een zeer brede verkenning nodig zijn van alle problemen en hulpvragen die spelen. In een ander geval is het wellicht voldoende om gericht binnen een specifiek (ander) domein informatie te zoeken over een inwoner.

Stap 3 Geef de betrokken inwoner de regie: informeer en vraag toestemming
Voor het verkrijgen van informatie uit een ander domein is vrijwel altijd de toestemming van de betrokken inwoner nodig. Toestemming vragen begint met informeren. Leg de inwoner uit:
- waarom het voor zijn hulpvraag nodig is om informatie bij elkaar te leggen, bestanden te raadplegen of overleg te voeren

- om welke informatie het gaat
- van wie deze informatie afkomstig is en/of wie er meedoen aan het overleg

Vraag de inwoner- nadat hij goed weet wat er gaat gebeuren- om toestemming voor de integrale gegevensverwerking. Geeft de inwoner geen toestemming, dan vindt geen integrale gegevensuitwisseling of overleg in het team plaats. Behalve als de uitzondering van Stap 4 zich voordoet.

Stap 4 Beoordeel of- i.v.m. ernst problematiek- toch integraal(bepaalde) informatie moet worden uitgewisseld In uitzonderingssituaties kan toch informatie vanuit andere domeinen uitgewisseld worden zónder dat er toestemming is. Zijn er aanwijzingen dat:

- de situatie van de inwoner of zijn gezin zeer ernstig is; en
- hij of zijn gezin dringend hulp nodig heeft; en
- dat deze hulp alleen goed kan worden geboden door integrale gegevensverwerking of integraaloverleg,

dan kan alles afwegend op grond van het leerstuk van het conflict van plichten/vitaal belang uiteindelijk worden besloten om toch integraalgegevens te verwerken of overleg te voeren (artikel6 lid 1 onderdeel d AVG).

Het gaat bij deze stap om een zorgvuldige afweging op casusniveau. Met andere woorden: er moet goed gekeken worden welke feiten erop wijzen dat de situatie ernstig is én het moet duidelijk zijn waarom integrale gegevensverwerking of overleg noodzakelijk is als middel om de situatie te verbeteren.

Bronvermelding: Onderstaand stappenplan is een bewerkte versie van het stappenplan uit De Kleine Gids. Privacy en beroepsgeheim in het sociale domein.

Bijlage 7 Privacy reglement email- en internetgebruik

http://decentrale.regelgeving.overheid.nl/cvdr/xhtmloutput/actueel/Nieuwegein/CVDR28423.html

Bijlage 8 Begrippen

In dit beleidskader worden verschillende begrippen geïntroduceerd met een zekere lading vanuit de privacy-wetgeving. Het gaat hierbij om:

- Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;
- Bijzondere persoonsgegevens: alle persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de, unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemand seksueel gedrag of seksuele gerichtheid.
- Verwerking: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;
- Verwerkingsverantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt;
- Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/ dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt;
- Bestand: elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is dan wel op functionele of geografische gronden is verspreid;
- Ontvanger: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de persoonsgegevens worden verstrekt. Overheidsinstanties die mogelijk persoonsgegevens ontvangen in het kader van een bijzonder onderzoek overeenkomstig het Unierecht of het lidstatelijke recht gelden echter niet als ontvangers; de verwerking van die gegevens door die overheidsinstanties strookt met de gegevensbeschermingsregels die op het betreffende verwerkingsdoel van toepassing zijn;
- Derde: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken;
- Toestemming van de betrokkene: elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt;

Bijlage 9 Activiteitenoverzicht en implementatie

Na vaststelling van het beleidsplan privacy zullen een aantal activiteiten worden opgepakt ter verdere uitwerking van het beleidsplan. In het schema staan de verschillende activiteiten opgesomd, onder wiens verantwoordelijkheid de activiteit valt en of het om incidentele of structurele activiteiten gaat.

Activiteit Verantwoordelijkheid Incidenteel/Structureel

Inrichten privacy office	Privacy office	Structureel
Inrichten en bijhouden van het register van verwerkingen en het overzicht verwerkersrelaties	Privacy office	Structureel
Passende technische maatregelen voor veilig gebruik persoonsgegevens conform artikel 25 AVG	Privacy office	Structureel
Inhaalslag tzv ontbrekende contracten of protocollen en het bijhouden van deze registers	Privacy office	Incidenteel
Werkinstructies opstellen voor: - Uitvoeren rechten van betrokkenen (Art 15 ev. AVG) - Behandelen bezwaren van betrokkenen (Art 21 AVG)	Afdelingen in overleg met privacy office	Incidenteel
Werkinstructies opstellen voor: - Opslaan persoonsgegevens in archieven - Cameratoezicht - Gebruik BSN - Datalekken - Omgaan met ID-bewijzen - Beheer van device - overig	Teammanagers	Incidenteel
Vaststellen takenpakket medewerkers en toegang tot bestanden (instroom, doorstroom en uitstroom)	Teammanagers	Structureel
Aanschaf beveiligde devices voor gebruik buitenshuis, inrichten en instrueren	Teammanagers die het aangaat	Structureel
Integratie van privacy- en veiligheidsbeleid in de jaarlijkse planning en controlcyclus	Teammanager (primair) Controller in overleg met privacy office (secund)	Structureel
Opstellen jaarlijks activiteitenplan bewust omgaan met persoonsgegevens	Teammanagers	Structureel
Opstellen communicatieplan Privacy en informatieveiligheid (intern en extern) en het uitvoeren van de communicatieactiviteiten	Communicatiemedewerker in overleg met privacy office	Structureel