GEMEENTEBLAD
Officiële uitgave van de gemeente Bunschoten
Nr. 108778
11 maart
2024

Privacybeleid 2020 van de gemeenten Bunschoten, Leusden, Nijkerk en Putten

1. AANLEIDING/INLEIDING

De digitalisering van onze samenleving vindt in rap tempo plaats. Steeds meer digitale informatie wordt gebruikt, gedeeld en aan elkaar gekoppeld. Organisaties, apparaten en netwerken worden met elkaar verbonden, ook bij gemeenten. Digitale technologie is op het werk en privé niet meer weg te denken en deze werelden lopen steeds meer door elkaar. Alles wordt slim, van slimme meters tot slimme steden, bovendien zal digitalisering steeds sneller gaan. Trends en ontwikkelingen zoals robotica, virtual reality, drones, 3D-printing, etc. zullen steeds verder geïntegreerd raken in de gemeentelijke processen. Aan deze ontwikkelingen kleven ook risico's. Zo staat de privacy vaak onder druk. Als de informatie op enig moment niet beschikbaar is, zijn we direct onthand. Alternatieven voor digitale gegevenswerking bestaan al bijna niet meer. Daarnaast zijn er dreigingen zoals cybercriminaliteit en onbedoelde inzage of aanpassing van de gegevens door onbevoegden. Wereldwijd is het aantal incidenten vanwege cybercriminaliteit de afgelopen jaren fors toegenomen.

Sinds 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing en is de Uitvoeringswet gegevensbescherming van kracht. Dat betekent dat op basis van de AVG dezelfde privacywetgeving geldt in de hele Europese Unie (EU).

De gemeenten Bunschoten, Leusden, Nijkerk en Putten (BLNP), werken sinds begin 2017 samen op het gebied van de bedrijfsvoering: ICT, HRM, Financiën en Juridische Zaken. Daarom hebben de colleges besloten om ook het privacybeleid gezamenlijk te ontwikkelen en dit -zo uniform mogelijk lokaal uit te voeren, in nauwe samenhang met het BLNP-brede Informatieveiligheidsbeleid.

Bescherming van persoonsgegevens is niet nieuw, maar in de AVG wordt een aantal zaken scherper geformuleerd zoals het recht van betrokkene om 'vergeten te worden', het recht om inzage in zijn/ haar persoonsgegevens te hebben, het recht om verwijdering of wijziging van persoonsgegevens en transparantie plus verantwoording vanuit de gemeente. Het correct en duurzaam inrichten en bijhouden van een register over alle verwerking van persoonsgegevens speelt hierbij een belangrijke rol. Maar ook onze contracten met externe partijen die voor ons persoonsgegevens verwerken moeten tegen het licht worden gehouden en indien nodig aangepast.

Aangezien zowel de Uitvoeringswet als de AVG de rechten en plichten zo goed als uitputtend beschrijven, is er weinig ruimte voor lokale beleidsruimte. Wel kunnen gemeenten op basis van de wetgeving eigen prioriteiten en doelstellingen formuleren. Deze beleidsnota voorziet daarin. Vanuit het belang van de bescherming van privacy en de wettelijke kaders komen wij in relatie tot informatiebeveiliging tot een organisatorische inbedding, waarbij de bescherming van privacy, de openheid naar onze inwoners en het belang van het maatwerk binnen de afwegingen die steeds gemaakt moeten worden in goede balans zijn met elkaar. De AVG is rechtmatig geformuleerd.
Rechtspraak en de Autoriteit Persoonsgegevens hebben afgelopen jaar een verhelderende rol gehad in de uitgangspunten. Dit beleid gaat uit van rechtmatigheid maar heeft door middel van een risico gebaseerde aanpak ook een rechtvaardige en doelmatige werking.

2. LEESWIJZER

Dit beleidsdocument bestaat uit een beschrijving van de manier waarop de BLNP-gemeenten toepassing zullen geven aan de AVG en aanverwante privacywetgeving.
Dit beleid bestaat daarnaast uit 10 bijlagen*. Wij adviseren u om eerst bijlage 1 en 2 door te nemen indien u niet bekend bent met de basisbegrippen uit de AVG en de governance BLNP.

Bijlage 1. Governance BLNP
Bijlage 2. Uitwerking begrippen AVG
Bijlage 3. Procedure Incidentmanagement en Respons Bijlage 4. Procedure DPIA
Bijlage 5. Procedure Rechten van Betrokkenen
Bijlage 6. Standaard verwerkersovereenkomst *(huidig format bijgevoegd)*
Bijlage 7. Kapstokbeleid privacy Sociaal Domein *(in ontwikkeling)*
Bijlage 8. Instructies Sociaal Domein (in ontwikkeling) Bijlage 9. Privacy by design *(in ontwikkeling)*

Bijlage 10. Verwerkingsregister *(zie website gemeente)*

In bijlage 1 worden de inrichting van de privacy-organisatie en de samenhang tussen sturing, uitvoering en verantwoording toegelicht. Deze bijlage gaat in op de samenhang tussen informatieveiligheid en privacybescherming. In bijlage 2, worden de kernbegrippen in de AVG en de verhouding van de AVG tot andere wetten beschreven. Bijlage 3 Urn 10 zijn documenten ter (praktische) uitvoering van de AVG.

*Op het moment van vaststellen van deze nota zijn nog niet alle gewenste privacy protocollen/ werkprocesaanpassingen en overige afspraken en documenten gereed. Deze zullen op een later moment als bijlagen aan het beleid worden toegevoegd. Dit beleidsdocument moet daarom worden beschouwd als een 'levend' document.

3. AANPAK PRIVACYBESCHERMING IN BLNP-VERBAND

De BLNP-gemeenten willen elkaar versterken door een gezamenlijke aanpak van privacyvraagstukken en daarvoor benodigde capaciteit, kennis en middelen zoveel mogelijk te delen. Zowel informatieveiligheid als privacybescherming zijn binnen het taakveld ICT belegd bij BLNP gastheergemeente Bunschoten, met de kwartiermaker ICT. De FG valt rechtspositioneel gezien onder de gemeente Bunschoten en de privacybeheerders onder de gemeente door wie zij zijn aangesteld. Zie ook Hoofstuk 9 en 10 en bijlage 1. De FG is aangesteld voor 32 uur en de privacybeheerders zijn aangesteld voor ieder 18 uur. Opleidingen en trainingen worden gezamenlijk verzorgd. Ook wordt in BLNP verband onderzoek gedaan naar de mogelijke aanschaf van een informatieveiligheid managementsysteem/ privacymanagementsysteem (ISMS). In het kader van de Baseline Informatiebeveiliging Overheden is het hanteren van een ISMS verplicht geworden.

Bescherming van persoonsgegevens is een onderwerp dat breed en diep in onze gemeentelijke organisaties aandacht verdient. Het raakt sterk aan informatiebeveiliging en maakt er onderdeel van uit. In lijn met informatiebeveiligingsbeleid wordt ook bij privacy een risico-gestuurde aanpak gehanteerd. Dat betekent dat op basis van periodieke analyse de risico's in beeld worden gebracht. En dat vervolgens op de hoogste risico's maatregelen worden genomen om die risico's in te perken. Deze aanpak past bij de wijze waarop het wetgevend kader in de AVG is ingericht. Een risico-gestuurde aanpak is in lijn met de BIO en zorgt voor een gedegen balans tussen risico's enerzijds en efficiëntie/ praktische uitvoerbaarheid anderzijds. De AVG geeft ruimte voor afweging door de professionals. Ook liggen verantwoordelijkheden en (proces)eigenaarschap laag in de organisaties. Richtlijnen voor afwegingen tussen hulp en zorg verlenen, ondersteuning bieden en gelijktijdig recht doen aan bescherming van persoonsgegevens zal in de praktijk van de komende jaren verder inhoud krijgen.

De AVG geeft gemeenten ook kaders voor verantwoording en controle. De colleges leggen verantwoording af aan hun gemeenteraad over de werking van dit beleidsdocument en daaruit voortkomende maatregelen. Naast dit beleid is onder meer een register van verwerkingen opgesteld en een (wettelijk verplichte) Functionaris voor de Gegevensbescherming (FG) aangesteld voor de vier gemeenten. De FG wordt ook voor de gemeenteraad in de BLNP-gemeenten aangewezen. De gemeenteraad is niet bevoegd tot het stellen van bindende voorschriften ten aanzien van de AVG aangezien deze Europese regelgeving betreft. De belangen die de AVG vertegenwoordigt, hebben voor de gemeenteraad uiteraard wel veel relevantie en maken deel uit van de kader stellende taak van de raad waar het gaat om het informeren en betrekken van burgers, partners waar de gemeente mee samenwerkt en van medewerkers bij privacybescherming en van de controlerende taak van de raad ten aanzien van de uitvoering van privacytaken en de verantwoording hierover door het college. Daarom wordt de gemeenteraad periodiek geïnformeerd door het college over actuele ontwikkelingen. Indien gewenst kan de gemeenteraad aanvullende privacyregels laten vaststellen. In Nijkerk heeft de gemeenteraad voor haar taken een privacywerkwijzer vastgesteld en gepubliceerd.

Gemeenten kennen meerdere overheidsorganen die als "verwerkingsverantwoordelijke" in de zin van de AVG worden aangemerkt voor de verwerking van persoonsgegevens. De burgemeester is verantwoordelijk voor alle gegevensverwerkingen die te maken hebben met diens openbare orde en veiligheidstaken en de raad is verantwoordelijk voor de verwerkingen door de griffie en de raadscommissies. Het college van burgemeester en wethouders is verantwoordelijk voor alle overige gegevensverwerkingen. Dit betekent dat de verplichte gemeentelijke FG voor elk van bovengenoemde overheidsorganen moet worden aangewezen en zijn aangemeld bij de Autoriteit persoonsgegevens.
Hetzelfde geldt overigens ook voor de FG van de gemeenschappelijke regelingen die als zelfstandig bestuursorgaan verwerkings- verantwoordelijke zijn, zoals de veiligheidsregio of de gemeenschappelijke regeling voor de belastingheffing.

4. BEGINSELEN PRIVACYBELEID

Het BLNP-brede privacybeleid heeft de volgende uitgangspunten die gebaseerd zijn op de AVG:
1. het is inzichtelijk in hoeverre en op welke manier persoonsgegevens worden gebruikt
2. het is duidelijk voor welk doel persoonsgegevens worden gebruikt
3. er worden niet te veel maar ook niet te weinig persoonsgegevens verwerkt
4. de gebruikte persoonsgegevens zijn juist en actueel
5. persoonsgegevens worden niet langer bewaard dan nodig
6. persoonsgegeven worden op een passende manier beveiligd

Deze uitgangspunten zijn van toepassing op al het gebruik van persoonsgegevens. Deze zes principes zijn leidend. Daarbij wordt benadrukt dat deze principes geen doel op zich zijn maar een onderdeel vormen van de werkzaamheden die de gemeente in het belang van haar burgers verricht. Deze principes maken echter altijd onderdeel uit van de te maken afwegingen binnen ambtelijke werkprocessen en van de bestuurlijke besluitvorming.

5. PRIVACY-PRINCIPES, DOELSTELLING EN STRATEGIE

Om de (informationele) privacy te waarborgen handelen wij vanuit de volgende principes:
1. Wij verwerken vooral voor onze inwoners en medewerkers veel persoonsgegevens waaronder ook bijzondere persoonsgegevens.
2. Wij zijn ons bewust van de maatschappelijke verantwoordelijkheid die dit met zich mee brengt.
3. Wij gaan zorgvuldig en vertrouwelijk om met persoonsgegevens en treffen passende beveiligingsmaatregelen.
4. Wij zijn transparant over het verzamelen, gebruik, opslaan en delen van persoonsgegevens.
5. Wij houden voortdurend rekening met de belangen van mensen bij de verwerking van hun persoonsgegevens. Wij hebben daarbij in het bijzonder oog voor kwetsbare groepen. Wij zoeken daarbij de ruimte op binnen de wettelijke kaders, zeker wanneer de zorg voor onze inwoners hierom vraagt. Wij zetten bij dilemma's de belangen van onze inwoners centraal en gaan wij pro actief het gesprek met hen aan.

De uitvoering van wettelijke taken van de BLNP-gemeenten, optimale dienstverlening en privacybescherming betekenen het constant zoeken naar een evenwichtige balans tussen deze principes. De BLNP-gemeenten streven naar een optimum, met risico oriëntatie en het moreel kompas als belangrijke ijkpunten.

De colleges van de BLNP-gemeenten gaan vanuit deze principes voor de volgende doelstelling:

'Wij geloven dat een goede privacybescherming, dienstverlening en werkbaarheid samen kunnen gaan. Waar dit botst en privacy moet wijken voor de uitvoering van onze taken, of omgekeerd, maken we de besluitvorming hierover transparant.'

Waar nodig zullen de BLNP-gemeenten zich verder verbeteren door middel van een aanpak die gebaseerd is op het identificeren, wegen en wegnemen van risico's waar dat binnen de verantwoordelijkheden en mogelijkheden van de gemeenten ligt en de werking hiervan jaarlijks te evalueren. In BLNP verband wordt onderzoek gedaan naar de mogelijke aanschaf van een informatieveiligheidmanagementsysteem/ privacy managementsysteem (ISMS). Door het inrichten van een ISMS en het uitvoeren van (verplichte) activiteiten kan aantoonbaar gemaakt worden dat voldoende aandacht wordt besteed aan informatiebeveiliging & privacybescherming. Dit vraagt om een professionele organisatiecultuur met professionele medewerkers. Om deze professionaliseringsslag te kunnen maken, wordt veel aandacht besteed aan bewustwording, kennisontwikkeling, beïnvloeding van gedrag en duidelijke informatie en instructies. Van medewerkers -en van proceseigenaren- wordt verwacht dat zij hun verantwoordelijkheden op het gebied van privacybescherming kennen en implementeren in hun werkzaamheden. Continu anticiperen en verbeteren is het uitgangspunt om goed te kunnen inspelen op steeds veranderende dreigingen.

De strategie om de doelstelling te bereiken is als volgt:
1. Het toepassen en verder optimaliseren van dit BLNP-brede privacybeleid en te blijven anticiperen op nieuwe maatschappelijke en technische ontwikkelingen;
2. Ruimte bieden voor dialoog en gezond verstand, zeker waar het gaat om kwetsbare mensen en andere zwaarwegende belangen;

3. Blijven werken aan privacybewustzijn binnen de vier organisaties en bij partijen waarmee de gemeenten samenwerken. Hieruit volgt dat:
   - De gemeentesecretarissen, proceseigenaren, leidinggevenden en (zelfsturende) teams sturen op privacybewustzijn binnen de vier gemeenten en op uniformiteit bij het BLNP-breed ontwikkelen en uitvoeren van privacybeleid. Hiermee wordt recht gedaan aan de uitgangspunten voor de BLNP bedrijfsvoerings-samenwerking: minder kwetsbaarheid, meer kwaliteit in dienstverlening, kennis delen, minder kosten, meer kansen voor medewerkers;
   - De collegeleden die verantwoordelijk zijn voor de gemeentelijke portefeuille informatieveiligheid en privacybescherming, overleggen minimaal tweemaal per jaar over het gevoerde privacybeleid en eventuele maatregelen om dit te verbeteren. Zij worden hierbij ondersteund door vier coördinerend proceseigenaren vanuit iedere gemeente en de vier privacybeheerders;
   - De privacybeheerders stellen in overleg met de vier coördinerend proceseigenaren een privacyjaarplan op waarover de FG-advies uitbrengt, voordat dit plan ter goedkeuring naar de gemeentesecretaris wordt gezonden;
   - De FG een jaarverslag over het voorgaande jaar stuurt naar de verwerkingsverantwoordelijken (raad, college en burgemeester);

4. Het toepassen en onderhouden van het genoemde onder 1, 2 en 3 met behulp van een informatieveiligeid-/ privacymanagement systeem (met een Privacy Plan-Do-Check-Act-cyclus), zodat de mogelijkheden die dit instrument biedt goed benut worden qua risicogebaseerd werken; Dit wordt momenteel onderzocht en hierover worden de colleges een aanvullend voorstel aangeboden.

6. RAAKVLAKKEN PRIVACYBELEID MET ANDERE BELEIDSTHEMA'S

Dit privacybeleid heeft veel raakvlakken met andere beleidsthema's. Juist vanwege die raakvlakken is het belangrijk om met elkaar in gesprek te gaan en privacy als kernwaarde mee te nemen bij het delen van visies en het verder ontwikkelen van beleid. Dit is vooral wezenlijk als deze visies of de te behartigen belangen tegengesteld zijn. De belangrijkste thema's waarbij dit kan spelen zijn:

1. Organisatie-inrichting en ontwikkeling:
   Keuzes die de privacy raken op het gebied van bijvoorbeeld Human Recourses, communicatie, fraudebestrijding, procesmanagement, intergemeentelijke of andere vormen van samenwerking;
2. <u>Dienstverlening:</u>
   De wijze waarop het privacybeleid wordt ingericht moet blijven aansluiten op de inrichting van de dienstverlening;
3. <u>Integriteitsbeleid:</u>
   Privacybeleid is wettelijk gekoppeld aan de beginselen van behoorlijk bestuur en is daarmee ondersteunend aan het gemeentelijk integriteitsbeleid;
4. <u>Kwaliteitsbeleid:</u>
   Het privacybeleid richt zich in belangrijke mate op het waarborgen van een kwalitatief goede administratieve organisatie als randvoorwaarde voor een klantgerichte en klantvriendelijke gemeente en goed werkgeverschap;
5. <u>Risicomanagement:</u>
   Het privacybeleid schept waarborgen om afbreuk- en aansprakelijkheidsrisico's op privacygebied tegen te gaan, voorkomt schending van het recht op privacy (onrechtmatige daad) en bevordert de continuïteit van werkzaamheden (profijt van checks and balances in plaats van inefficiëntie en ergernis door onduidelijkheden);
6. <u>Informatiebeheer:</u>
   Het privacybeleid onderschrijft de noodzaak tot een goed (en waar mogelijk of gewenst BLNP breed georganiseerd) informatiebeheer en het juist vastleggen en toegankelijke houden van de gemeentelijke informatie.

7. TRANSPARANTIE EN INFORMATIEVOORZIENING EXTERN /INTERN

De AVG zet in op uitbreiding van de privacyrechten van burgers en verlangt van de verwerkingsverantwoordelijken dat zij transparant zijn over de verwerkingen en dat de verwerkingen controleerbaar zijn. Voor een goede informatievoorziening over het toepassen van de AVG is het daarom van belang dat het privacybeleid gepubliceerd wordt. Over het kunnen uitoefenen van hun rechten door betrokkenen vindt u meer in bijlage 5. Het register van verwerking van persoonsgegevens en de privacyverklaring zijn voor iedereen te raadplegen via de gemeentewebsites

Bewustwording binnen de organisaties is nodig voor het slagen van privacybescherming. Bij de uitvoering van werkzaamheden is het belangrijk om te onderkennen wat risico's zijn uit het oogpunt van privacy en hoe daar mee om te gaan. Zonder dit besef zou er alleen gestuurd kunnen worden met hard ingeregelde geboden en verboden en toetsing daarop. Dit is niet werkbaar en niet gewenst. Het privacy risicobewustzijn wordt bij degenen die binnen de organisaties met persoonsgegevens te maken hebben (vrijwel iedereen) vooral aangesproken via voorlichting, vorming en een goede onderlinge interactie.
Van reële voorvallen, vragen en incidenten wordt meer geleerd dan van het zonder nadenken volgen van regels. De AVG biedt vanwege de risico gebaseerde aanpak ook mogelijkheid om keuzes te maken. Sturen op sociale controle, bijvoorbeeld over veilig mailen of bellen, en actieve voorlichting binnen teams stimuleren het privacybewustzijn maakt al deel uit van het BLNP-brede Informatieveiligheidsbeleid.

Periodiek worden de organisaties via informatiebijeenkomsten en/ of publicaties op intranet geïnformeerd over de ontwikkelingen op het gebied van informatieveiligheid en privacybescherming. Waar nodig kunnen aanvullende voorzieningen qua informatieveiligheid en privacybescherming voor nieuwe-medewerkers worden ingezet ten behoeve van het privacybewustzijn en kennis.

8. GOVERNANCE INFORMATIEVEILIGHEID & PRIVACYBESCHERMING

Om een goede naleving van privacyregelgeving te kunnen borgen binnen de organisaties, is het noodzakelijk om naast de sturing op en verantwoording over het privacybeleid ook de verdeling van taken en verantwoordelijkheden binnen de gemeentelijke organisatie goed in te richten. Dit geheel wordt samengevat als "governance". De governance richt zich ook op de samenwerking binnen Gemeenschappelijke Regelingen en andere samenwerkingsverbanden en op de samenhang met andere onderwerpen, met name met het gemeentebreed informatieveiligheidsbeleid, dat verder gaat dan privacybescherming alleen.

Omdat er veel raakvlakken zijn tussen informatieveiligheid en privacybescherming, is besloten om voor informatieveiligheid en privacybescherming één governancedocument te hanteren, (zie bijlage 1). Hierdoor wordt de samenhang tussen sturing op, uitvoering van en verantwoording over het gevoerde beleid met betrekking tot deze twee taakgebieden inzichtelijk gemaakt. Ook blijkt hieruit waar lokale verschillen zijn, bijvoorbeeld qua personele uitgangspunten, organisatiestructuur en deelnemingen in BV's.

9. GOVERNANCE UITGELICHT: DE FUNCTIONARIS GEGEVENSBESCHERMING

Eén FG voor vier gemeenten

De FG ziet binnen de vier gemeenten toe op de naleving van de AVG en het hierop gebaseerde privacybeleid en heeft een adviserende rol bij DPIA's (Data Protection Impact Assessments: gegevensbeschermingseffectbeoordeling), onderzoeken met betrekking tot privacy-aspecten bij privacygevoelige ontwikkelingen. De FG stemt zo nodig af en werkt samen met de Autoriteit Persoonsgegevens.

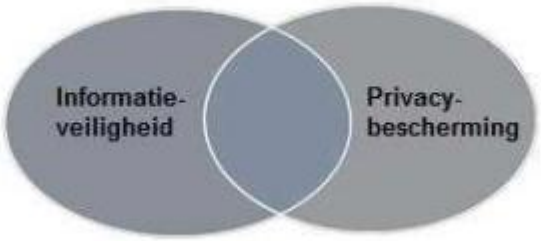
De colleges van Bunschoten, Leusden, Nijkerk en Putten hebben samen één FG en voldoen daarmee aan de verplichting in artikel 37 AVG. De positie van de FG staat beschreven in artikel 38 van de AVG. Dit artikel borgt dat de FG zijn taken onafhankelijk kan verrichten. De taken van de FG staan beschreven in artikel 39 van de AVG, onder meer het informeren en adviseren van het bestuur en de medewerkers over de AVG. In BLNP-verband verricht de FG ook taken voor de rekenkamercommissies, adviescommissies voor de bezwaarschriften, de ombudsman van de gemeenten Bunschoten, Nijkerk en Putten, de heffingsambtenaren (voor de taken die bij de gemeente berusten) en ambtenaren van de burgerlijke stand (BABS-en) en leerplichtambtenaren. Zoals genoemd in H3 wordt de FG wordt ook voor de gemeenteraden van de BLNP-gemeenten aangewezen. (Afzonderlijk voorstel)

Bijlage 1 bij privacybeleid 2020 van de gemeenten Bunschoten, Leusden, Nijkerk en Putten

Governance Informatieveiligheid en Privacy (IP) gemeente putten

1. Inleiding
In het privacybeleid van de gemeenten Bunschoten, Leusden, Nijkerk en Putten staan de beleidsuitgang5Punten voor de BLNP-samenwerking op het gebied van privacybescherming vermeld en in de bij dit beleid behorende bijlage 2, Uitwerking AVG, zijn de normen en kader voor het omgaan met persoonsgegevens verder uitgewerkt. In het informatieveiligheidsbeleid van deze gemeenten zijn normen en kaders gegeven om informatieverwerking -waaronder ook de verwerking van persoonsgegevens- veilig te houden. Dit governance document heeft als doel om de samenhang tussen sturing op, uitvoering van en verantwoording over het gevoerde beleid met betrekking tol deze twee taakgebieden inzichtelijk en transparant te maken.

1.1. Relatie informatieveiligheidsbeleid - privacybeleid
Informatieveiligheid en privacybescherming, zijn termen die soms door elkaar worden gebruikt. Informatieveiligheid en privacybescherming vallen echter niet één op één samen. Ze hebben een gemeenschappelijk raakvlak en beide ook een eigen domein daarbuiten. Dit is weergegeven in de onderstaande afbeelding.



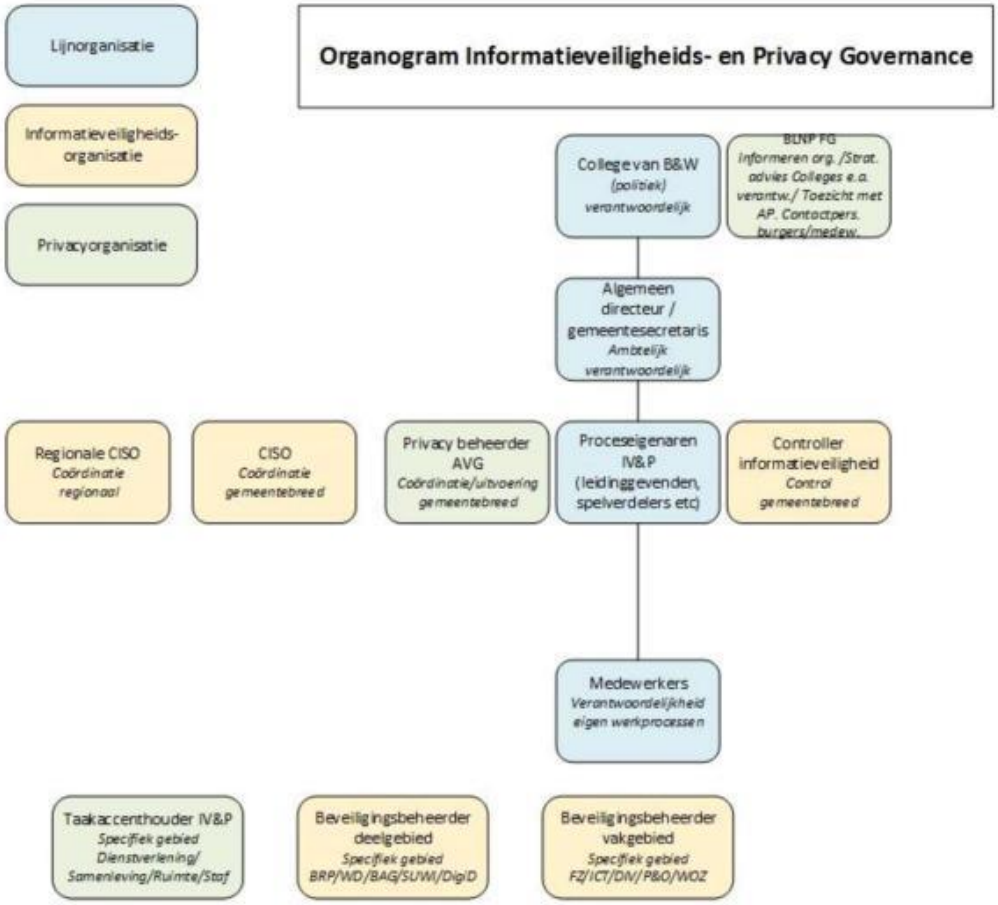
Adequate informatieveiligheid is een voorwaarde voor de privacywet- en regelgeving en als zodanig benoemd in de AVG. Dan gaat het om de verwerking van persoonsgegevens. Binnen informatieveiligheid kan zich een beveiligingsincident voordoen dat geclassificeerd wordt als datalek, omdat er persoonsgegevens bij betrokken zijn. In dat geval is de privacywetgeving van toepassing.

Informatieveiligheid heeft echter een veel bredere scope dan persoonsgegevens. Het gaat om de bescherming van alle data tegen aantasting van integriteit, vertrouwelijkheid en beschikbaarheid. Privacybescherming gaat daarnaast niet alleen over de beveiliging van persoonsgegevens tegen inbreuken, maar ook over de juiste verwerking van persoonsgegevens onder de voorwaarden zoals deze zijn vastgelegd in de privacywet- en regelgeving. Een belangrijk thema is de toegang van een burger tot zijn of haar persoonsgegevens en de mogelijkheid om deze gegevens of het gebruik ervan te corrigeren.

Het informatieveiligheidsbeleid en het privacy beleid van de gemeenten Bunschoten, Leusden, Nijkerk en Putten vormen samen een tweeluik over informatieveiligheid & privacybescherming.

2. Organisatie
Voor kaderstelling en uitvoering van zowel het informatieveiligheids- als het privacybeleid is een heldere inrichting van de organisatie nodig, met een duidelijke afbakening van verantwoordelijkheden, taken en bevoegdheden. In onderstaand schema zijn de verschillende actoren (instanties en functionarissen) weergegeven die een rol en een verantwoordelijkheid hebben in de sturing en implementatie van het informatieveiligheids- en/of privacybeleid.

De begrippen privacy en bescherming van persoonsgegevens worden vaak -ook in dit document door elkaar gebruikt bij het dienen van hetzelfde doel: het beschermen van persoonsgegevens en het eerbiedigen van de persoonlijke levenssfeer van natuurlijke personen.



2.1. Verantwoordelijkheidsniveaus
Binnen de gemeenten worden de volgende verantwoordelijkheids- en takenniveaus met betrekking tot informatieveiligheid en privacybescherming onderscheiden:

2.1.1. Beleidsbepalende, regisserende en coördinerende verantwoordelijkheden op organisatieniveau
Het College van B&W van de gemeenten is als eigenaar van gemeentelijke informatieprocessen en (informatie)systemen verantwoordelijk voor een passend niveau van informatieveiligheid en privacybescherming. Het college stelt de kaders op basis van Europese en landelijke wet- en regelgeving en landelijke normenkaders. Het college is verantwoordelijk voor een duidelijk te volgen informatieveiligheids- en privacybeleid en stimuleert het management van de organisatieonderdelen om beveiligings- en privacy maatregelen te nemen. Als eigenaar van informatie en (informatie)systemen kan het college verantwoordelijkheden op het gebied van beveiliging en privacy waar nodig verder mandateren aan de portefeuillehouders informatieveiligheid, de gemeentesecretaris en aan te wijzen medewerkers. Daarbij is functiescheiding een aandachtspunt evenals het sturen op privacy bewustzijn binnen de organisaties, waarbij zoveel mogelijk recht gedaan wordt aan de uitgangspunten voor de BLNP-bedrijfsvoering samenwerking: minder kwetsbaarheid, meer kwaliteit in dienstverlening, kennis delen, minder kosten, meer kansen voor medewerkers.

2.1.1.1 Portefeuillehouders Informatieveiligheid en Privacy
De positie van "verwerkingsverantwoordelijke" berust op grond van de AVG bij de bestuursorganen college, burgemeester en gemeenteraad. Het college is verantwoordelijk voor de meeste verwerkingen van persoonsgegevens (zie register van verwerkingen op de gemeentewebsites).
Omwille van de collegiale verantwoordelijkheid, vindt ten minste 2 x per jaar een BLNP-breed afstemmingsoverleg plaats tussen portefeuillehouders informatieveiligheid en privacy over het gevoerde privacybeleid en eventuele maatregelen om dit te verbeteren. Hierbij worden de portefeuillehouders ondersteund door de vier CISO's, de vier privacybeheerders en de coördinerend proceseigenaren uit de **BLNP**- gemeenten.

2.1.1.2 Gemandateerde verantwoordelijkheden en taken van de gemeentesecretaris
De gemandateerde verantwoordelijkheid voor informatieveiligheid en privacybescherming van het college en de burgemeester ligt bij de gemeentesecretaris. Deze stelt met het managementteam en/of aangewezen functionarissen binnen de organisatie, het gewenste niveau van informatieveiligheid en privacybescherming vast voor de gemeente. De privacy- en beveiligingseisen worden per bedrijfsproces vastgesteld. De gemeentesecretaris is verantwoordelijk voor de juiste implementatie van de privacybescherming en de beveiliging in de bedrijfsprocessen en de in- en externe (informatie)systemen.

De gemeentesecretaris heeft daarmee in ieder geval de volgende verantwoordelijkheden:
- Het aanwijzen van een CISO, een privacybeheerder, proceseigenaren privacy en een controller informatieveiligheid;
- Het laten opstellen van strategische en operationele beleidskaders en het sturen op informatieveiligheid en privacybescherming
- Periodiek evalueren van de beleidskaders en deze bijstellen waar nodig;
- Het (laten) controleren of de getroffen maatregelen overeenstemmen met de eisen en of deze maatregelen voldoende bescherming bieden;
- Het beleggen van de verantwoordelijkheid voor informatieveiligheidscomponenten en -systemen;
- Het inrichten van functiescheiding tussen beleidsbepalende, uitvoerende en controlerende taken met betrekking tot informatieveiligheid en privacybescherming.

2.1.1.3 Proceseigenaren, de verantwoordelijken op afdelings- en teamniveau
De door de gemeentesecretaris aangewezen coördinerend proceseigenaren zijn verantwoordelijk voor de (informatie)veiligheid en privacybescherming binnen de afdelingen/teams. Dit omvat zowel de personele capaciteit, bedrijfsprocessen als -systemen. Dit kunnen zowel afdelingshoofden/ leidinggevenden, teamleiders, als spelverdelers of anderszins verantwoordelijken zijn.

Proceseigenaren hebben in ieder geval de volgende verantwoordelijkheden:
- Het implementeren van het informatieveiligheids- en privacybeleid en de bijbehorende richtlijnen en maatregelen en het uitdragen van het informatieveiligheidsbeleid en het privacybeleid binnen de afdeling/het team;
- Het sturen op beveiligingsbewustzijn, op bedrijfscontinuïteit en op naleving van regels en richtlijnen (gedrag en risicobewustzijn);
- Het rapporteren, via de CISO/privacybeheerder, over compliance van informatieveiligheid en privacybescherming aan wet- en regelgeving en algemeen beleid van de gemeente in de P&C rapportages.
- Het (laten) uitvoeren van maatregelen uit de informatieveiligheidsanalyse die op de afdeling/team van toepassing zijn, waaronder DPIA's (Data Protection Impact Assessments) oftewel gegevensbeschermingseffectbeoordelingen;
- Op basis van een expliciete risicoafweging (laten) opstellen van betrouwbaarheidseisen voor de informatiesystemen;
- Het selecteren, implementeren en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen;
- Binnen de vier gemeenten wordt door de gemeentesecretaris één proceseigenaar aangewezen die fungeert als coördinerend proceseigenaar namens de betreffende gemeente, die deelneemt aan BLNP-brede overleggen rond privacybescherming, waaronder het BLNP-brede overleg tussen de Portefeuillehouders Informatieveiligheid en Privacybeheerders dat 2 maal per jaar plaatsvindt.

2.1.1.4 Chief Information Security Officer (CISO)
Deze functie is op organisatieniveau verantwoordelijk voor het actueel houden van het informatieveiligheidsbeleid, het coördineren van de uitvoering van het beleid, het adviseren bij projecten, het beheersen van risico's, evenals het opstellen van rapportages.

De CISO heeft in ieder geval de volgende verantwoordelijkheden:
- Informeert de FG wanneer zich een datalek of beveiligingsincident voordoet;
- Rapporteert rechtstreeks aan de gemeentesecretaris en het bestuur;
- Coördineert het opstellen en actualiseren van informatieveiligheidsbeleid;
- Stelt de informatieveiligheidsanalyse op en zorgt voor de actualisatie hiervan;
- Coördineert de prioritering van informatieveiligheidsmaatregelen uit de informatieveiligheidsanalyse en de uitvoering van het actieplan informatieveiligheid;
- Stelt een afstemmingsmechanisme op voor overleg en rapportage met betrekking tot informatieveiligheid;
- Ondersteunt de gemeentesecretaris en de afdelingsmanagers met kennis over informatieveiligheid, zodat zij hun verantwoordelijkheid voor de betrouwbaarheid van de informatievoorziening juist kunnen invullen;

- Is aanspreekpunt voor medewerkers van de gemeente over het onderwerp informatieveiligheid;
- Volgt de externe invloeden die van invloed zijn op het informatieveiligheidsbeleid en de informatieveiligheidsanalyse;
- Bevordert het beveiligingsbewustzijn in de organisatie;
- Houdt de registratie van informatiebeveiligingsincidenten bij in een incidentenregister en is verantwoordelijk voor de juiste afhandeling en evaluatie van incidenten;
- Rapporteert over de informatieveiligheid van de gemeente in de P&C managementrapportages. Hierbij bundelt de CISO de deelbijdragen van het afdelingsmanagement.

2.1.1.5 Regionale Chief Information Security Officer (Regionale CISO)
Naast de inrichting van de functie gemeentelijke CISO hebben de gemeenten Bunschoten, Nijkerk, Leusden en Putten een regionale CISO-functie ingericht. Deze regionale CISO voert de coördinatie over overkoepelende aangelegenheden die zich voordoen in BLNP verband, in overleg met de FG waar het bescherming van persoonsgegevens betreft en met de vier CISO's die op gemeentelijk niveau zijn aangewezen. Hiermee wordt invulling gegeven aan een eenduidig BLNP-informatieveiligheidsbeleid en een efficiënte uitwerking van het beleid.

2.1.1.6 Privacybeheerder
De privacybeheerder functioneert op uitvoeringsniveau (ten behoeve van het lokale management/afdelingen/teams) en is de rechterhand van de portefeuillehouder privacy en de verwerkingsverantwoordelijken (college, burgemeester, raad). Eén van de kerntaken van de privacybeheerder is om management/proceseigenaren te adviseren over een privacybestendige uitvoering van gegevensverwerkingen. Eén van de lokale privcaybeheerders wordt in onderling overleg aangewezen als coördinerend privacybeheerder BLNP. De coördinerend privacybeheerder initieert het gezamenlijk met de andere lokale privacybeheerders opstellen van een privacyjaarplan en een lange termijnplanning en heeft regelmatig afstemming met de Functionaris

Gegevensbescherming over de status van de voortgang van privacy-compliance/initiatieven/projecten. Verder heeft iedere privacybeheerder in ieder geval de volgende verantwoordelijkheden:
- Beoordelen van de verwerking van persoonsgegevens, tegen de achtergrond van de kaders van privacywetgeving en -beleid, adviseert de organisatie, bij wijzigingen in de bedrijfsvoering of de procesuitvoering en voert -zonodig- een DPIA uit.
- Als adviserend lid deelnemen aan programma's en projecten waarvan het resultaat gevolgen kan hebben voor de wijze van verwerking van persoonsgegevens, waaronder het BLNP-brede privacyoverleg, dat naast de privacybeheerders bestaat uit: kwartiermaker ICT/(optioneel), FG (in ieder geval maandelijks), regionale CISO's (optioneel).
- De privacybeheerder heeft verder als taak:
  a) de uitleg van de privacy voorschriften in de AVG en in de sectorale wetgeving;
  b) coördineren van de privacy werkzaamheden;
  c) coördineren, samenvoegen en openbaar maken van de registers van gegevensverwerkingen op basis van informatie die wordt aangeleverd door de organisatieonderdelen van de gemeenten;
  d) coördineren van verzoeken voor de uitoefening van de rechten van betrokkenen ten aanzien van persoonsgegevens, zoals deze zijn beschreven in de AVG en adviseren van de proceseigenaar over de afhandeling hiervan;
  e) rapporteert -aansluitend bij andere gemeentelijke controlcycli- en zoveel mogelijk in BLNP verband aan de (eind)verantwoordelijken (coördinerend proceseigenaar, gemeentesecretaris, portefeuillehouder privacy, college), en stuurt dit rapport ter kennisname naar de FG, die waar nodig, zijn advies zal uitbrengen aan de colleges;
  f) richt in overleg met de regionale CISO en FG procedures in voor het afhandelen van datalekken waarbij persoonsgegevens betrokken zijn en neemt deel aan de incidentenafhandeling volgens het protocol datalekken, onder toezicht van BLNP- CISO en FG;
  g) beheer en onderhoud van de standaarddocumenten die in BLNP-verband zijn ontwikkeld voor het privacybeleid, procedures zoals verwerkersovereenkomsten, convenanten en reglementen;
  h) advisering en ondersteuning bij het besluitvormingsproces en het afsluiten van verwerkersovereenkomsten en convenanten en de vaststelling van reglementen;
  i) Verzorgt de meldingen en intrekkingen van meldingen bij de Autoriteit Persoonsgegevens (AP);
  j) creëren van bewustzijn rondom de verwerking van privacygevoelige persoonsgegevens en daarbij horende risico's.

2.1.1.7 Functionaris voor de gegevensbescherming (FG)
De aanstelling van een Functionaris Gegevensbescherming (FG) is op grond van de Algemene Verordening Gegevensbescherming (AVG) verplicht. De BLNP-gemeenten stellen gezamenlijk een FG aan. De FG is de interne toezichthouder op de verwerking van persoonsgegevens binnen de organisatie. De

FG houdt binnen de organisatie toezicht op de toepassing en naleving van de Algemene Verordening Gegevensbescherming (AVG). De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie. Bij organisaties met een FG stelt de Autoriteit Persoonsgegevens (AP) zich terughoudend op als toezichthouder.

De FG heeft in ieder geval de volgende taken en verantwoordelijkheden:
- Het informeren en adviseren van de gemeenten en de verwerkers die namens de gemeente persoonsgegevens verwerken over hun verplichtingen uit hoofde van de AVG en andere EU wet en regelgeving en nationale bepalingen omtrent gegevensbescherming (geen advies ten aanzien van casussen);
- Het toezien op naleving van AVG, en andere EU wet- en regelgeving en nationale bepalingen omtrent gegevensbescherming,
- Adviseren over datalekken -waar nodig rechtstreeks- aan directeur/secretaris en aan de verwerkingsverantwoordelijke(n);
- en hierover Het toezien op naleving van het gemeentelijke beleid of de verplichtingen van de verwerker met betrekking tot de bescherming van persoonsgegevens;
- Het toezien op toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het bij de verwerking betrokken personeel en de betreffende audits;
- Het geven van advies met betrekking tot de Data Protection Impact Assessment (DPIA) en het toezien of de uitvoering daarvan in overeenstemming is met de AVG;
- Het samenwerken met de AP, en optreden als contactpunt voor de AP.

2.1.1.8 De controller informatieveiligheid (CI)
Deze rol is op organisatieniveau verantwoordelijk voor het verbijzonderde toezicht op de naleving van het informatieveiligheidsbeleid en de realisatie van voorgenomen veiligheidsmaatregelen en adviseert bij escalatie van beveiligingsincidenten. De CI rapporteert aan directeur/ gemeentesecretaris en aan het college B&W

De *controller informatieveiligheid* heeft in ieder geval de volgende taken en verantwoordelijkheden:
- Het (laten) organiseren van de periodieke toetsing op de juiste naleving, de werking, de effectiviteit en de kwaliteit van de maatregelen ten aanzien van informatieveiligheid. Het principe hierbij is dat de toetsing binnen een bepaald domein plaatsvindt door een beveiligingsbeheerder van een ander domein en visa versa.
- De controle op de voortgang van het uitvoeren van de maatregelen uit de informatieveiligheidsanalyse en het actieplan informatieveiligheid;
- De controle op de periodieke actualisatie van het informatieveiligheidsbeleid en de informatieveiligheidsanalyse;
- Toetsen/bewaken van het niveau van informatieveiligheid;
- Toetsing van evaluatieproces van beveiligingsincidenten.

De rol van controller informatiebeveiliging heeft bij twee specifieke deelgebieden een wettelijk voorgeschreven officiële benaming. Namelijk op het gebied van reisdocumenten en van rijbewijzen: *Beveiligingsfunctionaris*

2.1.1.9 De beveiligingsbeheerder
Deze rol is verantwoordelijk voor het beheer, de coördinatie en advies ten aanzien van de informatieveiligheid van specifieke gegevensverzamelingen. In wetgeving worden verschillende benamingen aan rollen gegeven voor veelal dezelfde taken en verantwoordelijkheden ten aanzien van specifieke gegevensverzamelingen. Om eenduidigheid in naamgeving te verkrijgen wordt in dit beleidsdocument de veiligheidsverantwoordelijkheid ten aanzien van een specifieke

gegevensverzameling toegewezen aan en gedefinieerd als beveiligingsbeheerder, aangevuld met de deelgebieden waarvoor een beveiligingsbeheerder is aangewezen.: BRP, Reisdocumenten* Rijbewijzen*, SUWI, BAG en DigiD. Daarnaast worden er beveiligingsbeheerders aangewezen op verschillende aspecten van de gemeentelijke bedrijfsvoering: Facilitaire Zaken, ICT, DIV, P&O en WOZ (GBLT).

De *beveiligingsbeheerder* heeft de volgende taken en verantwoordelijkheden:
- Is - voor het toegewezen deelgebied - verantwoordelijk voor het geheel van activiteiten gericht op de toepassing en naleving van de maatregelen en procedures die voortkomen uit het informatieveiligheidsbeleid, inclusief de maatregelen die voortkomen uit de audit en (zelf)evaluatie voor het betreffende onderdeel. Hieronder vallen:
  - de voorbereiding en coördinatie van audits en (zelf)evaluaties
  - de preventie en detectie van beveiligingsincidenten en het geven van een adequate respons
  - het coördineren van de toepassing van specifieke wet- en regelgeving
  - het rapporteren aan de CISO en de controller informatieveiligheid.

* Specifieke verplichte beveiligingsbeheerdersrollen:
- *Autorisatiebevoegde Reisdocumenten/Aanvraagstations*: Verantwoordelijk voor het beheer van de autorisaties voor de reisdocumentenmodules (RAAS en aanvraagstations).
- *Autorisatiebevoegde Rijbewijzen*: Verantwoordelijk voor het beheer van de autorisaties voor rijbewijzen, inclusief aanmelding RDW.
- *Security Officer SUWI*: Beheert beveiligingsprocedures en -maatregelen in het kader van Suwinet, overeenkomstig wettelijke eisen. De Security Officer bevordert en adviseert over de beveiliging van Suwinet en ziet er daarnaast op toe dat de maatregelen worden nageleefd. Ook adviseert de Security Officer medewerkers en management, doet voorstellen tot implementatie c.q. aanpassing van plannen op het gebied van de beveiliging van Suwinet en evalueert de uitkomsten van verbetermaatregelen.

De Security Officer verzorgt minimaal tweemaal per jaar een rapportage met betrekking tot de beveiligingsstatus van Suwinet aan het hoogste management en/of college. De Security Officer SUWI vraagt daarnaast meerdere keren per jaar een rapportage op bij het BKWI over het gebruik van Suwinet door de gemeente.

2.1.1.10 Eerste aanspreekpunten privacy
Deze rol is verantwoordelijk voor het beheer, de coördinatie en advies ten aanzien van privacybescherming van specifieke gegevensverzamelingen. In de organisatie is het eigenaarschap van bepaalde processen en systemen waarmee wordt gewerkt toegedeeld aan bepaalde "proceseigenaren". Naast deze proceseigenaren zijn mensen aangewezen met een signalerende rol ten aanzien van privacybescherming binnen een proces. Wanneer er ontwikkelingen zijn waarbij privacybescherming een rol speelt zijn zij eerste aanspreekpunt. Wanneer het complexe zaken betreft, schakelt de Aaanspreekpunt privacy de privacybeheerder in.

Het Aanspreekpunt privacy is - voor het toegewezen deelgebied - verantwoordelijk voor het geheel van activiteiten gericht op de toepassing en naleving van de maatregelen en procedures die voortkomen uit het privacybeleid, inclusief de maatregelen die voortkomen uit de audit en (zelf)evaluatie. Hieronder vallen:
- de preventie en detectie van beveiligingsincidenten en het geven van een adequate respons;
- het coördineren van de toepassing van specifieke wet- en regelgeving;
- het rapporteren aan de Privacy Officer en de FG.
- Aanmelden nieuwe verwerkingen van persoonsgegevens bij de Privacybeheerder,;
- Wijzigingen in de verwerking van persoonsgegevens melden bij de Privacybeheerder;
- De aanvraag, inbreng van inhoudelijke, functionele kennis, en uitvoer en effectueren van de resultaten van de DPIA;
- In behandeling nemen van verzoeken om inzage, correctie en verzet ten aanzien van persoonsgegevens;
- Afsluiten, beheren en actualiseren van verwerkersovereenkomsten;
- Aanwijzen decentraal contactpersoon informatieveiligheid en privacy;
- In het geval van een veiligheidsincident, inventariseren van feiten en omstandigheden;
- Het implementeren van adviezen uit veiligheidsrapportages en DPIA's;
- Het uitdragen van het informatieveiligheidsbeleid en het privacybeleid binnen de afdeling;

2.1.2 De teams binnen de BLNP gemeenten
De teams zijn eigenaar van en integraal verantwoordelijk voor de (informatie)veiligheid en privacy van de informatieprocessen en -systemen binnen hun team. Alle medewerkers dragen verantwoordelijkheid voor de informatieveiligheid en gegevensbescherming van de activiteiten die behoren tot hun eigen functie en taken.

Ieder team/ afdeling/ cluster heeft in ieder geval de volgende verantwoordelijkheden:
- Het waarborgen van privacy en bescherming van persoonsgegevens conform relevante wet- en regelgeving, bijv:
  - het bijhouden van verwerkingen en verwerkersovereenkomsten
  - het classificeren van opgeslagen data in applicaties en gegevensverzamelingen
  - het bieden van transparantie (informatieplicht) over het verwerken van gegevens in processen en aanvraagformulieren
  - het uitoefenen van rechten van betrokkenen vanuit AVG, bijvoorbeeld inzageverzoek

- Het (laten) uitvoeren van maatregelen/ adviezen ten aanzien van privacy (bijv. uit een DPIA)
- Opdrachtgeven tot en toezien op het uitvoeren van periodieke beveiligingsaudits;
- Het (laten) uitvoeren van maatregelen uit de informatieveiligheidsanalyse die op de afdeling van toepassing zijn;

- Het rapporteren, via de coördinator informatieveiligheid, over compliance (voldoen) aan wet- en regelgeving en algemeen beleid van de gemeente in de P&C rapportages.

2.1.2.1 Team(s) ICT
Het team ICT, waarvan systeembeheer deel uitmaakt, beheert de werkplekken, serverplatformen, lokale netwerken, Wi-Fi verbindingen, externe netwerkverbindingen (zoals Gemnet en Suwinet) en verzorgt het technische (wijzigings)beheer van databases, bedrijfsapplicaties en kantoorautomatiseringshulpmiddelen. Het is medeverantwoordelijk voor alle technische aansluitingen op andere ketenpartners en landelijke voorzieningen. Daarnaast zijn zij verantwoordelijk voor de implementatie van ICT-technische beveiligingsmaatregelen. Verantwoording over het gevoerde beheer van de getroffen beveiligingsmaatregelen wordt aan de procesverantwoordelijken voor (informatie)systemen afgelegd.

Afdeling overstijgende (informatie)systemen binnen de gemeente worden onder de verantwoordelijkheid van het team ICT gefaciliteerd en onderhouden. Deze systemen, die door meer dan één gemeentelijk organisatieonderdeel worden gebruikt, bevatten gegevens die door meerdere organisatieonderdelen worden vastgelegd. Voor ieder afdeling overstijgend (informatie)systeem wijst de gemeentesecretaris een organisatieonderdeel dat of medewerker aan die verantwoordelijk is voor de gehele gegevensverzameling of het (informatie)systeem. Indien de gemeentesecretaris hier niet expliciet toe besluit behoort deze verantwoordelijkheid aan het team ICT.

De procesverantwoordelijke van een afdeling overstijgend (informatie)systeem draagt er zorg voor dat bij het gebruik ervan de wettelijke eisen en de gemeentelijke voorschriften worden nageleefd en dat de verantwoordelijkheden voor beveiliging voor alle betrokken partijen duidelijk omschreven zijn.

2.1.2.2 Team(s) facilitaire zaken
Het team facilitaire zaken is verantwoordelijk voor de fysieke veiligheid in en rond het gebouw, fysieke toegangsbeveiliging, de kantoorinrichting (archiefkasten, kluizen enzovoort) en contacten en contracten met externe partijen die voorzien in fysieke veiligheid, zoals alarmopvolging, bewaking en beveiliging. De beveiligingsbeheerder FZ neemt namens het team deel aan het informatieveiligheidsoverleg.

2.1.2.3 Het team P&O (binnen de BLNP gemeenten)
Het team P&O is verantwoordelijk voor het beheer en de advisering ten aanzien personele en de organieke veiligheidsaspecten binnen de organisatie. De beveiligingsbeheerder P&O neemt deel aan het informatieveiligheidsoverleg namens team P&O.

2.1.2.4 Functioneel en gegevensbeheerder
Functioneel- en gegevensbeheerders zijn verantwoordelijk voor het geheel van activiteiten gericht op het ondersteunen van de informatiesystemen en de waarborging van continuïteit aan de gebruikerszijde van de informatievoorziening en voor het geheel van activiteiten gericht op de inhoudelijke kwaliteitszorg betreffende het gegevens verzamelen, de gegevensverwerking en de informatievoorziening.

2.2. Afstemming Informatieveiligheid en Privacy (IVP)
Het is belangrijk dat er tussen de taakvelden informatieveiligheid en privacybescherming afstemming gezocht wordt. Voor de afstemming zijn er verschillende overlegvormen beschreven op lokaal en regionaal niveau. Tussen informatieveiligheid en gegevensbescherming wordt zowel binnen de individuele gemeenten als binnen BLNP verbinding gezocht om zoveel mogelijk met elkaar op te trekken en kennis te delen. Om deze reden zijn de hierna volgende regionale overleggen ingesteld. Wanneer nodig wordt verbinding gezocht tussen de verschillende overlegvormen, zoals wanneer het de beveiliging van persoonsgegevens betreft. Hieronder wordt per overleg aangegeven wie daarbij aanwezig is en wat de onderwerpen zijn die tijdens deze overleggen besproken worden.

2.2.1. Lokaal overleg informatieveiligheid
De CISO is voorzitter van het overleg informatieveiligheid dat 2 tot 4 maal per jaar bij elkaar komt. Bij dit overleg zijn aanwezig:
- De CISO
- De controller Informatieveiligheid;
- Beveiligingsbeheerders t.a.v.: BRP/Waardedocumenten, BAG, SUWI en DigiD;
- Beveiligingsbeheerders t.a.v.: FZ, ICT, P&O, DIV en WOZ;
- De privacybeheerder;
- Agendaleden: gemeentesecretaris, afdelingsmanager, teamleider of specialist.

Onderwerpen:
- Voortgang uitvoering maatregelen uit de informatieveiligheidsanalyse c.q. uit het actieplan Informatieveiligheid;
- Beveiligingsincidenten;

- Planning en voorbereiding van audits, controles en zelfevaluaties;
- Evaluatie en actualisatie informatieveiligheidsbeleid en de informatieveiligheidsanalyse;
- Controle of de invulling van de rollen in de governance structuur nog actueel is.

2.2.2. Lokaal overleg privacybescherming
De privacybeheerder is voorzitter van het overleg gegevensbescherming dat 2 tot 4 maal per jaar bij elkaar komt. Bij dit overleg zijn aanwezig:
- De privacybeheerder
- De Functionaris Gegevensbescherming
- De Aaanspreekpunt privacy
- De CISO
- Agendaleden: gemeentesecretaris, afdelingsmanager, teamleider of specialist.

Onderwerpen:
- Voortgang uitvoering maatregelen die voortvloeien uit het privacybeleid;
- De uitvoering van Privacy Impact Assessment (PIA);
- Datalekken;
- Evaluatie en actualisatie privacybeleid;
- Controle of de invulling van de rollen in de governance structuur nog actueel is.

2.2.3. Regionaal CISO overleg
Voor informatieveiligheid komen de vier CISO's met de regionale CISO samen voor overleg en afstemming wat in regionaal verband wordt opgepakt. Dit overleg is de plek om ervaring en kennis over informatieveiligheid uit te wisselen. Deze overleggen worden eventueel aangevuld met specialisten die vanwege hun expertise betrokken zijn.

2.2.4. Regionaal privacy overleg
Voor privacybescherming komen de vier privacybeheerders, samen met de FG en de regionale CISO, om de regionale stand van zaken te bespreken en afstemming te vinden over het vervolg. Ook wordt tijdens deze overleggen kennis over privacy wet- en regelgeving uitgewisseld. Deze overleggen worden eventueel aangevuld met specialisten die vanwege hun expertise betrokken zijn.

2.3. Kernteam incidenten/ calamiteiten
Voor interne crisisbeheersing dient een kernteam informatieveiligheid geïnstalleerd te zijn. Dit team komt uitsluitend bij elkaar in geval van grote incidenten/calamiteiten. Dit team bestaat uit:
- De coördinator informatieveiligheid/ CISO (voorzitter);
- De privacybeheerder
- De controller informatiebeveiliging;
- De beveiligingsbeheerder ICT;
- De afdelingsmanager verantwoordelijk voor de afdeling waar het incident heeft plaatsgevonden;
- Indien nodig: relevante experts, medewerkers en gemeentesecretaris;
- De teamleider communicatie.
- Agendalid: de FG

Voor nadere informatie over de afhandeling van incidenten en/ of datalekken: zie bijlage procedure Incidentmanagement en Respons

3. Rollen en namen BLNP

1	Het beheren van het verwerkingsregister				
	• De (proces)eigenaar van de betreffende persoonsgegevens binnen de organisatie is verantwoordelijk voor de actualiteit van de verwerkingen van zijn organisatieonderdeel in het register. De eigenaar is de medewerker dan wel het aanspreekpunt van het organisatieonderdeel dat de betreffende persoonsgegevens verwerkt. • De privacybeheerder is verantwoordelijk voor het beheer van het organisatiebrede overzicht van alle persoonsverwerkingen. • De Functionaris Gegevensbescherming ziet toe op het invullen van de verantwoordelijkheden van de eigenaar en van de privacy beheerder en ziet toe op de integriteit, vertrouwelijkheid en beschikbaarheid van het register en de (eventuele) melding van de verwerking bij de privacybeheerder en de FG.				
		PB	(P)E	Ciso	FG
	Melden nieuwe verwerkingen en aanleveren tekst voor verwerkingsregister bij FG en PB.		✓		
	Actualisering verwerkingsregister		✓		
	Coördinatie en beheer verwerkingsregister	✓			
	Toetsing op juistheid en volledigheid verwerkingsregister				✓

2	Registratie, beheer en actualisatie van verwerkersovereenkomsten				
	• De eigenaar van de betreffende persoonsgegevens binnen de organisatie is verantwoordelijk voor het afsluiten, beheren en actualiseren van een verwerkersovereenkomst. De eigenaar is de medewerker dan wel het aanspreekpunt van het organisatieonderdeel dat de betreffende persoonsgegevens verwerkt. • De privacybeheerder is verantwoordelijk voor de beschikbaarheid van een actuele model verwerkersovereenkomst. De privacybeheerder geeft daarnaast advies aan de eigenaar over het afsluiten van de verwerkersovereenkomst qua over specifieke voorwaarden/ bepalingen en ondersteunt bij vraagstukken met de derde partij (de verwerker). • De CISO geeft advies over het afsluiten van de verwerkersovereenkomst rondom informatieveiligheid over specifieke voorwaarden en ondersteunt bij vraagstukken met de derde partij (de verwerker) qua specifieke beveiligingsmaatregelen. • De Functionaris Gegevensbescherming ziet toe op het invullen van de verantwoordelijkheden van de eigenaar en de privacybeheerder. De FG ziet er op toe dat volgens de (Europese) privacywetgeving wordt gehandeld en ziet tevens toe op de integriteit, vertrouwelijkheid en beschikbaarheid van de centrale registratie				
		PB	PE	Ciso	FG
	Actualiseren en beheren model verwerkersovereenkomst	✓			
	Advies t.a.v. werken met verwerkers en verwerkersovereenkomsten	✓		✓	
	Afsluiten verwerkers-overeenkomsten en archivering		✓		
	Toezicht op registratie verwerkers en verwerkersovereenkomsten.				✓

3	Afhandeling veiligheidsincidenten / datalekken
	• De eigenaar van de betreffende persoonsgegevens binnen de organisatie is verantwoordelijk voor de interne melding, de informatievoorziening, registratie, eventuele externe melding en de interne en eventueel externe communicatie rond het incident. • De CISO en de privacy beheerder zijn verantwoordelijk voor inhoudelijke ondersteuning van de eigenaar bij het doorlopen van de procedure die in werking treedt bij een veiligheidsincident, het opstellen van een compact verslag gedurende het proces en de centrale registratie van het incident. Zij geven alsmede advies aan de eigenaar gedurende het doorlopen van de procedure. • De FG wordt z.s.m. geïnformeerd gedurende de incidentenprocedure en de eerste analyse. In geval van dilemma's wordt z.s.m. afstemming gezocht met gemeentesecretaris (en indien van toepassing bestuurder). • De FG is tevens verantwoordelijk voor de toetsing op implementatie van de adviezen uit de rapportages. • De eigenaar is tevens verantwoordelijk voor de implementatie van adviezen die voortkomen uit onderzoek en opgenomen in de rapportage.

		PB	PE	Ciso	FG
	Inventarisatie feiten en omstandigheden	✓	✓	✓	
	Opstellen verslag en analyse	✓		✓	
	Verstrekken advies	✓		✓	✓
	Opstellen rapportage			✓	
	Implementeren van adviezen uit rapportages		✓		
	Toetsing van geïmplementeerde adviezen uit rapportages				✓

4	Advies/ voorlichting aan de organisatie
	• De privacybeheerder, FG en CISO geven gevraagd en ongevraagd advies aan de organisatie (medewerkers en management) en bestuur met betrekking tot privacyvraagstukken. • De eigenaar is verantwoordelijk voor aandacht voor informatieveiligheid en privacy op de afdeling.

		PB	PE	Ciso	FG
	(On)gevraagd advies verlenen aan bestuur, management en medewerkers m.b.t. privacyvraagstukken	✓		✓	✓
	Voorlichting en communicatie over privacy (bewustwording) aan de organisatie	✓		✓	✓
	Continue aandacht voor informatieveiligheid en privacy op de afdeling		✓		

5	Ontwikkelen en beheer van procedures, formats en beleid
	• De eigenaar is verantwoordelijk voor de uitvoering van het beleid ten aanzien van de betreffende persoonsgegevens die onder zijn verantwoordelijkheid vallen. • De privacybeheerder, CISO en FG zijn verantwoordelijk voor de ontwikkeling, het beheer, de optimalisatie en de interne en externe communicatie rond procedures, formats en beleid met betrekking tot privacy/ informatieveiligheid. • De FG is verantwoordelijk voor de toetsing op de uitvoer van het beleid.

		PB	PE	Ciso	FG
	De ontwikkeling, het beheer, de optimalisatie en de interne en externe communicatie rond procedures, formats en beleid met betrekking tot privacy		✓		
	Ten uitvoer brengen van het beleid		✓		
	Het beheer en de archivering van procedures, formats en beleid m.b.t. privacy/informatieveiligheid	✓		✓	
	Toezicht op de kwaliteit, archivering, communicatie en toepassing van procedures, formats en beleid				✓

6	Uitvoeren DPIA
	• De eigenaar is verantwoordelijk voor de aanvraag, inbreng van inhoudelijke, functionele kennis, en uitvoer en effectueren van de resultaten van de PIA. • De privacybeheerder is verantwoordelijk voor inhoudelijke ondersteuning van de eigenaar bij het doorlopen van de procedure die in werking treedt bij uitvoeren van een PIA. De privacy-beheerder geeft daarnaast, samen met de CISO, advies aan de eigenaar gedurende het doorlopen van de procedure. • De FG adviseert bij het doorlopen van de PIA procedure .

		PB	PE	Ciso	FG
	Initiëren / aanvragen DPIA		✓		✓
	Uitvoeren DPIA	✓			
	Inhoudelijk en procedurele ondersteuning van de eigenaar bij doorlopen van de DPIA procedure	✓		✓	
	Opstellen verslag, inclusief aanbevelingen, verwerken en archiveren van de resultaten DPIA	✓			
	Uitvoeren acties/implementeren maatregelen voortkomend uit DPIA		✓		
	Toetsen uitgevoerde maatregelen/ acties en de effecten hiervan.				✓

7	Klachtafhandeling
	• De eigenaar is verantwoordelijk voor het initiëren, het doorlopen, het verzorgen van interne en externe communicatie en afsluiten van de klachtafhandelingsprocedure. Dit eventueel in samenwerking met de gemeentelijke klachtencoördinatoren. • De privacybeheerder en de CISO zijn verantwoordelijk voor de inbreng van inhoudelijke en procedurele kennis die nodig is voor het doorlopen van de klachtafhandelingsprocedure. • De Functionaris Gegevensbescherming ziet toe op de kwaliteit en de correcte afhandeling van de klacht.

		PB	PE	Ciso	FG
	Het initiëren, doorlopen, verzorgen van interne en externe communicatie		✓		

	en afsluiten van de klachtafhandelingsprocedure.				
	Inbreng van inhoudelijke en procedurele kennis	✓		✓	
	Toetsen op kwaliteit en correcte afhandeling van klacht				✓

8	Afhandelen verzoek rechten van betrokkenen m.b.t. persoonsgegevens				
	• De eigenaar is verantwoordelijk voor de afhandeling van verzoeken van de rechten van betrokkenen met betrekking tot de persoonsgegevens die onder zijn verantwoordelijkheid vallen. • De privacybeheerder coördineert de afdelingsoverstijgende verzoeken van betrokkenen. Dit betekent dat deze de verzoeken in ontvangst neemt, het verzoek uitzet binnen de organisatie, verzamelt informatie en een terugkoppeling geeft aan de betrokkene. • De Functionaris Gegevensbescherming ziet toe op de afhandeling van de verzoeken van betrokkenen.				
		PB	PE	Ciso	FG
	Verzoek uitvoeren		✓		
	Indien afdelingsoverstijgend: uitzetten vraag binnen de organisatie, verzamelen informatie en terugkoppeling naar aanvrager	✓			
	Procedureel en inhoudelijk ondersteunen bij de procedure	✓			
	Verantwoordelijk voor het bijhouden van de procedure voor afhandelingen verzoeken, het voorlichten en bewust maken binnen de organisatie van de rechten van betrokkenen	✓			
	Toezicht op het doorlopen van de procedure				✓

4. Rollen en namen BLNP

4.1 rollen en namen Bunschoten

Beveiligingsrollen	Naam	Vervanger
1. Chief Information Security Officer (CISO)	[redacted]	CISO LNP-verband
2. Controller Informatieveiligheid		
3. Functionaris Gegevensbescherming		
4. Coordinerend Proces Eigenaar		
5. Privacybeheerder		Privacybeheerder LNP-verband
6. Beveiligingsbeheerder BRP		
7. Beveiligingsbeheerder Waardedocumenten		
8. Beveiligingsbeheerder Suwinet		
9. Beveiligingsbeheerder BAG		
10. Beveiligingsbeheerder WOZ		
11. Beveiligingsbeheerder DigiD		
12. Beveiligingsbeheerder ICT		[redacted]
13. Beveiligingsbeheerder P&O		
14. Beveiligingsbeheerder DIV		[redacted]
15. Beveiligingsbeheerder FZ		
16. Aanspreekpunten teams		
17. Algemeen Contactpersoon Informatiebeveiliging (ACIB)		
18. Vertrouwd Contactpersoon Informatiebeveiliging (VCIB)		[redacted]

4.2 rollen en namen Leusden

Beveiligingsrollen	Naam	Vervanger
19. Chief Information Security Officer (CISO)	[redacted]	
20. Controller Informatieveiligheid		
21. Functionaris Gegevensbescherming		
22. Privacybeheerder		Privacybeheerder BNP
23. Coordinerend Proces Eigenaar		
24. Beveiligingsbeheerder BRP		
25. Beveiligingsbeheerder Waardedocumenten		
26. Beveiligingsbeheerder Suwinet		
27. Beveiligingsbeheerder BAG		
28. Beveiligingsbeheerder WOZ		
29. Beveiligingsbeheerder DigiD		
30. Beveiligingsbeheerder ICT		

4.3 rollen en namen Nijkerk

Beveiligingsrollen	Naam	Vervanger
36. Chief Information Security Officer (CISO)	[redacted]	[redacted] (Bunschoten)
37. Controller Informatieveiligheid		
38. Functionaris Gegevensbescherming		
39. Privacybeheerder		Privacybeheerder BLP
40. Coördinerend proceseigenaar		
41. Beveiligingsbeheerder BRP		
42. Beveiligingsbeheerder Waardedocumenten		
43. Beveiligingsbeheerder Suwinet		[redacted]
44. Beveiligingsbeheerder BAG		[redacted]
45. Beveiligingsbeheerder BGT		
46. Beveiligingsbeheerder WOZ		
47. Beveiligingsbeheerder DigiD		[redacted]
48. Beveiligingsbeheerder ICT		[redacted]
49. Beveiligingsbeheerder P&O		[redacted]
50. Beveiligingsbeheerder DIV		
51. Beveiligingsbeheerder FZ		[redacted]
Aanspreekpunten privacy zelfsturende teams		
52. adviseurs dagelijks leven		
53. adviseurs zelfredzaamheid arbeidsmarkt		
54. backoffice sociaal domein		
55. bedrijfsvoering		
56. burgerzaken		
57. communicatie		
58. dagelijks beheer uitvoerend		
59. dagelijks beheer zelforganiserend		
60. facilitaire dienstverlening		
61. financiën		
62. HRM		
63. informatiebeheer		
64. Informatisering		
65. inkomen		

4.4: rollen en namen Putten

Beveiligingsrollen	Naam	Vervanger
82. Chief Information Security Officer (CISO)	Vacant	Binnen BLNP
83. Controller Informatieveiligheid		
84. Functionaris Gegevensbescherming	[redacted]	
85. Privacybeheerder		Privacybeheerder BLN
86. Beveiligingsbeheerder BRP		[redacted]
87. Beveiligingsbeheerder Waardedocumenten		
88. Beveiligingsbeheerder Suwinet		
89. Beveiligingsbeheerder BAG		
90. Beveiligingsbeheerder WOZ		
91. Beveiligingsbeheerder DigiD		
92. Beveiligingsbeheerder ICT		
93. Beveiligingsbeheerder P&O		
94. Beveiligingsbeheerder DIV		
95. Beveiligingsbeheerder FZ		
96. Algemeen Contactpersoon Informatiebeveiliging (ACIB)		
97. Vertrouwd Contactpersoon Informatiebeveiliging (VCIB)		

Bijlage 2 bij privacybeleid 2019-2020 van de gemeenten Bunschoten, Leusden, Nijkerk en Putten

Uitwerking AVG

Doel: toelichting kernbegrippen en verhouding AVG tot relevante wetten

1. Kernbegrippen AVG

De kernbegrippen binnen de AVG zijn:

1. Toepasselijkheid AVG
2. Verantwoordingsplicht/ Accountability
3. Persoonsgegevens
4. Verwerking (van persoonsgegevens)
5. Verwerkingsgrondslagen
6. Doelbinding
7. Verwerkingsverantwoordelijke en verwerker
8. Betrokkene
9. Bijzondere en gevoelige persoonsgegevens
10. Bewaartermijnen
11 Privacy by design en privacy by default
12 Data Protection Impact Assesment
13 Anonimiseren/ Pseudnonimisering

1. Toepasselijkheid AVG

De AVG is van toepassing op 'de gehele of gedeeltelijke geautomatiseerde verwerking, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen'). Kortgezegd betekent dit dat de AVG in ieder geval van toepassing is wanneer de gemeente persoonsgegevens per computer verwerkt.
Maar de AVG is ook van toepassing in situaties waarin deze handmatig worden verwerkt en er dus géén sprake is van een geautomatiseerde verwerking. Als er bijvoorbeeld sprake is van geschreven gespreksnotities van ambtenaren over inwoners die verzameld zijn in mappen, is de AVG ook van toepassing.[1]

2. Verantwoordingsplicht
Feitelijk is de verantwoordingsplicht ('accountability') het centrale begrip binnen de AVG. Het is opgenomen in artikel 5 AVG. Het eerste lid van artikel 5 somt de zes basisbeginselen van de AVG op, zie Hoofdstuk 4 van het Privacybeleid. De essentie van de verantwoordingsplicht is dat de verwerkingsverantwoordelijke (in de meeste gevallen het college van burgemeester en wethouders) verantwoordelijk is voor het naleven van deze beginselen en deze naleving kan aantonen. De gemeente moet actief aantonen dat ze aan de AVG en haar beginselen voldoet. Er is sprake van een omgekeerde bewijslast. Het is niet zo dat een betrokkene of de toezichthouder moet aantonen dat de gemeente niet aan een verplichting voldoet. Dit alles vraagt om een actieve houding van de gemeente, waarbij desgevraagd aan toezichthouder of betrokkene kan worden aangetoond dat de beginselen worden nageleefd. De invulling van de verantwoordingsplicht komt met name tot uiting in:
Beschermings/beveiligingsbeleid
Verwerkingsregister
Privacy Impact Assessments (ook wel: Data Protection Impact Assesment)
Procedure datalekken

3. Persoonsgegevens
De AVG formuleert persoonsgegevens als volgt: "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".

1) Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming (https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/handleidingalgemeneverordeninggeg evensbescherming.pdf)

Een postcode alleen is niet direct herleidbaar tot een natuurlijk persoon. Er is meer informatie nodig om dat te kunnen doen. Bijvoorbeeld een huisnummer. Of de verwerkingsverantwoordelijke de middelen en de mogelijkheden heeft om iemand te kunnen identificeren, is niet doorslaggevend. Er moet gekeken worden naar alle middelen waarvan redelijkerwijs te verwachten valt dat zij worden gebruikt door de verwerkingsverantwoordelijke of door een andere persoon. Een kenteken is een persoonsgegeven, zelfs ook wanneer de verwerkingsverantwoordelijke zelf geen toegang heeft tot de bestanden van de Rijksdienst voor het Wegverkeer *(Handboek AVG A. Engelfriet* e.a, *p.20).*

4. Verwerking (van persoonsgegevens)
De AVG definieert een verwerking in artikel 4 lid 2 als volgt: 'een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde handelingen, 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.' Kort gezegd: iedere handeling met persoonsgegevens geldt als verwerken. De lijst die wordt opgesomd in de definitie is niet limitatief.

5. Verwerkingsgrondslagen
Een van de eisen die de AVG stelt is dat persoonsgegevens rechtmatig worden verwerkt. Artikel 6 AVG geeft in dat kader de grondslagen voor verwerking. Persoonsgegevens mogen alleen worden verwerkt indien één van die grondslagen van toepassing is. Hieronder worden de belangrijkste grondslagen besproken.

5.1 Toestemming (art 6 lid 1 AVG)
Betrokkene heeft toestemming gegeven voor het verwerken van persoonsgegeven voor een of meer specifieke doeleinden. De AVG verstaat onder toestemming '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.'

In deze definitie zitten een aantal elementen: van belang is dat de toestemming in vrijheid is gegeven. Als er een afhankelijke relatie (bijvoorbeeld tussen werkgever en werknemer, of binnen de gemeente in het sociaal domein) bestaat tussen degene die toestemming geeft en degene die de persoonsgegevens wil gebruiken, is er een grote kans dat de gegeven toestemming niet in vrijheid is gegeven. In de praktijk zal van een vrije toestemming niet snel sprake zijn gezien de vaak aanwezige afhankelijkheidsrelatie tussen de gemeente en de betrokkene.

Verder dient de toestemming specifiek geïnformeerd te zijn. Dat wil zeggen: deze mag niet te ruim en algemeen geformuleerd zijn, en het moet voor de betrokkene duidelijk zijn welke persoonsgegevens voor welke doeleinden verwerkt worden. Toestemming is ondubbelzinnig wanneer er geen onduidelijkheid kan bestaan of de betrokkene daadwerkelijk toestemming heeft gegeven voor een specifieke verwerking. Ook moet kunnen worden aangetoond dat de betrokkene toestemming heeft gegeven. Dat betekent duidelijk, specifiek en schriftelijk vastleggen. Indien dit digitaal wordt gevraagd moet een actieve opt-in handeling worden verricht. Concreet: het op een webformulier vooraf aanvinken van het hokje 'ik verleen toestemming' is niet toegestaan. Betrokken moet zelf het vinkje zetten.

Een gegeven toestemming kan te allen tijde worden ingetrokken. Dit betekent dat er dan geen grondslag voor verwerking overblijft. Toestemming is dus een risicovolle grondslag. Er zullen modellen voor de verschillende vormen van toestemming worden gemaakt. Deze zullen aan dit beleid worden toegevoegd. Toestemming moet in ieder geval altijd schriftelijk geschieden. Daarbij moet steeds blijken dat betrokkene weet waarvoor hij toestemming heeft gegeven.

5.2 Wettelijke verplichting
Het verwerken van persoonsgegevens is noodzakelijk om aan een wettelijke verplichting te voldoen. Een voorbeeld: de Participatiewet verplicht het college van burgemeester en wethouders in bepaalde gevallen om (persoons)gegevens te verstrekken aan instanties, zoals bijvoorbeeld de belastingdienst. Om aan deze verplichting te voldoen is het noodzakelijk dat het collegegegevens verwerkt.

5.3 Publiekrechtelijke taak
De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag. Hiervan is bijvoorbeeld sprake als de gemeente een bij wet geregelde - publiekrechtelijke - taak uitvoert. Er moet sprake zijn van een typische overheidstaak. Een voorbeeld hiervan is het beslissen op een aanvraag voor een maatwerkvoorziening op grond van de Wmo 2015.

6. Doelbinding

Persoonsgegevens mogen uitsluitend voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld. Let wel: verzamelen is ook verwerken! Voordat aan verwerking van persoonsgegevens gedacht kan worden, moet er dus eerst duidelijkheid zijn over een specifiek en concreet, dus precies omschreven doel. Wanneer er geen wettelijke grondslag is, is er in ieder geval geen sprake van een gerechtvaardigd doel.

Vervolgens kan de gemeente deze persoonsgegevens verder verwerken (bijvoorbeeld door deze te verstrekken aan derden). Dat mag uitsluitend wanneer het doel voor deze verdere verwerking verenigbaar is met het oorspronkelijke doel. Dit wordt *doe/binding* genoemd.

Een voorbeeld: een zorgverzekeraar mag persoonsgegevens van een klant verzamelen in het kader van de uitvoering van de verzekeringsovereenkomst. Stel dat de klant medicijnen declareert die een relatie hebben met het hebben van overgewicht. De verzekeringsmaatschappij mag vervolgens de gegeven van de klant niet doorgeven (verkopen) aan bedrijven die dieetproducten verkopen. Het doel waarvoor de persoonsgegevens in de eerste instantie verzameld zijn door de zorgverzekeraar (het uitvoeren van de zorgpolis) komt immers niet overeen met het nieuwe doel (het verkopen van profielen van klanten).

Bedenk dat de noodzaak van het hebben van een specifiek en gerechtvaardigd doel ook geldt binnen de gemeente. Voor het uitvoeren van een wet als de Wmo 2015 mogen persoonsgegevens verzameld worden: er is een wettelijke grondslag en een welbepaald doel. Maar die persoonsgegevens mogen vervolgens niet zomaar voor andere doeleinden worden gebruikt, bijvoorbeeld voor het koppelen met Jeugdwetbestanden . Er moet op zo'n moment altijd eerst worden nagegaan of er sprake is van verenigbaar doel.

7. Verwerkingsverantwoordelijke en verwerker
Binnen de AVG wordt onderscheid gemaakt tussen:
- de verwerkingsverantwoordelijke
- de verwerker

7.1 Verwerkingsverantwoordelijke
De verwerkingsverantwoordelijke is de entiteit (natuurlijke persoon, rechtspersoon, instantie of het (bestuursorgaan) die/dat het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. De verwerkingsverantwoordelijke dient te zorgen voor passende waarborgen voor het naleven van de AVG. Dat de waarborgen zijn ingesteld moet door de verwerkingsverantwoordelijke kunnen worden aangetoond. In feite is de verwerkingsverantwoordelijke aanspreekbaar op het handhaven van de zes basisbeginselen binnen de AVG (zie punt 1.2).
De doelen die worden vastgesteld moeten welbepaald, uitdrukkelijk omschreven en Gerechtvaardigd zijn. Met middelen worden alle gereedschappen en andere middelen bedoeld waarmee een verwerking wordt uitgevoerd, bijvoorbeeld software.

Wie is verwerkingsverantwoordelijke? In de meeste gevallen zal dat het college van burgemeester en wethouders zijn, vooropgesteld dat het college doel en middelen van de verwerking vaststelt. Maar ook de burgemeester of de raad kunnen verwerkingsverantwoordelijke zijn. De burgemeester als het bijvoorbeeld gaat om zijn taken op het gebied van openbare orde en veiligheid.

De AVG kent 'gezamenlijke verwerkingsverantwoordelijken' (art 26 AVG). In dat geval stellen twee of meer verwerkingsverantwoordelijken doel en middelen van de verwerking vast. In die gevallen waarbij de gemeente betrokken is bij samenwerkingsovereenkomsten (b.v. ketensamenwerking) waarbij er sprake is van meerdere verwerkingsverantwoordelijken, dan dient te worden vastgesteld welke partij welke verantwoordelijkheden op zich neemt.

7.2 Verwerker
Een verwerker[2] is een entiteit (natuurlijke persoon, rechtspersoon, instantie of (bestuurs)orgaan) die een verwerking uitvoert binnen het doel en middelen die de verwerkingsverantwoordelijke heeft vastgesteld. Een verwerker heeft geen zeggenschap over de wijze van verwerken, en werkt strikt onder instructies en in opdracht van de verwerkingsverantwoordelijke. Een verwerker neemt geen beslissingen over het gebruik van de gegevens, de verstrekking aan derden en andere ontvangers, de duur van de opslag van de gegevens etc.

7.3 Onderscheid verwerkingsverantwoordelijke en verwerker (toelichting)

2) Artikel 4 lid 8 AVG samen met artikel 28 AVG

Een verwerkersverantwoordelijke is in beginsel aansprakelijk voor alle schade, ongeacht of die door hem of de verwerker wordt veroorzaakt, (art 82 AVG) .Een verwerker is daarentegen slechts aansprakelijk voor de schade die door een verwerking is veroorzaakt wanneer bij die verwerking niet is voldaan aan de specifieke verplichtingen binnen de AVG die zijn gericht tot verwerkers (bijvoorbeeld het toepassen van een passend beveiligingsniveau), of wanneer de schade is ontstaan doordat de verwerker zich niet aan de instructies van verwerkingsverantwoordelijke houdt.

Van belang is om te benoemen dat een betrokkene zowel verwerker als verwerkingsverantwoordelijke voor het geheel van de schade kan aanspreken. Er bestaat tussen verwerker en verwerkersverantwoordelijke wel een mogelijkheid om de vergoede schade te verhalen op de ander. Het is om meerdere redenen van groot belang om vast te stellen wie verwerkingsverantwoordelijke is en wie verwerker. De AVG legt de meeste verantwoordelijkheden bij de verwerkingsverantwoordelijke neer: deze is aanspreekbaar op de verantwoordingsplicht, is aanspreekpunt voor wat betreft de rechten van betrokkenen, is aanspreekbaar op (het melden van) datalekken etc. Zodra een verwerker zelf het doel en de middelen van de verwerking gaat vaststellen wordt deze automatisch verwerkingsverantwoordelijke, zie art. 28 lid 10 AVG.

Wanneer het college een verwerker inschakelt voor het verwerken van persoonsgegevens, dient er een verwerkersovereenkomst gemaakt te worden. Deze moet schriftelijk of elektronisch worden aangegaan. De AVG bepaalt in artikel 28 welke zaken in zo'n verwerkersovereenkomst opgenomen moeten worden (zie ook bijlage 6). Onder andere het nemen van passende technische en organisatorische maatregelen.

De BLNP-gemeenten hanteren een standaard-verwerkersovereenkomst die afkomstig is, of gebaseerd is op het model van de VNG/IBD. In alle gevallen wordt deze standaard overeenkomst aangeboden aan verwerkers en wordt deze opgenomen in het aanbestedingstraject.

8. Betrokkene
De betrokkene is de natuurlijke persoon op wie de persoonsgegevens betrekking hebben. Met de invoering van de AVG krijgen burgers meer mogelijkheden om voor zichzelf op te komen bij de verwerking van hun gegevens. Hun rechten en plichten worden namelijk versterkt en uitgebreid in de artikelen 13 t/m 22 AVG. De betrokkene kan zich voor het inroepen van zijn rechten wenden tot de verwerkingsverantwoordelijke, in de meeste gevallen het college van burgemeester en wethouders. De rechten en plichten gelden voor eenieder waarvan persoonsgegevens worden verwerkt door de gemeente. Het gaat dus niet alleen om de rechten en plichten van de inwoners van de gemeente. De AVG spreekt daarom over de rechten van betrokkenen. Bijlage 5 bij dit privacybeleid geeft een uiteenzetting van de verschillende rechten. In het kort:
- recht op informatie
- recht op inzage
- recht op rectificatie
- recht op vergetelheid
- recht op beperking van de verwerking
- recht op bezwaar

De gemeente moet transparant zijn over de verwerking van persoonsgegevens. Het moet voor betrokkenen duidelijk zijn in hoeverre en op welke manier er persoonsgegevens worden verwerkt. Alle communicatie richting betrokkene moet begrijpelijk zijn, ook met betrekking tot de rechten van betrokkenen. De gedachte hierachter is dat de betrokkene beter in staat is om in te schatten wat er met zijn gegevens gebeurt en eventueel actie kan ondernemen. Een uitwerking hiervan is de privacyverklaring die de gemeenten op de website hebben gepubliceerd.

9. Bijzondere en gevoelige persoonsgegevens
Bijzondere persoonsgegevens en gevoelige persoonsgegevens spelen een belangrijke rol. Bijzonder persoonsgegevens worden in de AVG geregeld, in de praktijk speelt ook het ruimere begrip 'gevoelige gegevens' een rol.

9.1 Bijzondere persoonsgegevens
Er worden in artikel 9 van de AVG een aantal categorieën van bijzondere persoonsgegevens gehanteerd, die extra privacygevoelig zijn. Het betreft: ras of etniciteit, politieke opvattingen, religie/levensbeschouwing, vakbondslidmaatschap, genetische gegevens, biometrische gegevens, gegevens over gezondheid, gegevens betreffende seksualiteit.

In principe is het verboden om deze gegevens te verwerken, tenzij. De AVG en de Uitvoeringswet AVG bepaalt in welke gevallen bijzondere of gevoelige gegevens verwerkt mogen worden. Er zijn uitzonderingen op dat verbod, bijvoorbeeld in het geval betrokkene uitdrukkelijke toestemming heeft gegeven, of in het geval de gemeente de gegevens moet verwerken voor het uitvoeren van een wettelijke taak,

zoals bijvoorbeeld de Wmo 2015. De gemeente dient uiterst zorgvuldig om te gaan met bijzondere persoonsgegevens.
Nieuw is dat genetische en biometrische gegevens tot de bijzondere persoonsgegevens worden gerekend. Bij biometrische gegevens moet gedacht worden aan een pasfoto op een rijbewijs of paspoort, of een vingerafdruk. Het wordt enkel gebruikt om iemand te identificeren. Ook hier geldt dus: verwerking is verboden, tenzij. De gemeente verwerkt biometrische gegevens enkel als dit nodig is voor het uitvoeren van een wettelijke taak (bv het uitgifte paspoort op grond van de Paspoortwet). Ook kunnen ze worden verwerkt voor beveiligingsdoeleinden, bijvoorbeeld voor de toegang tot het gemeentekantoor.

Net als onder de Wbp behoren strafrechtelijke gegevens tot de bijzondere persoonsgegevens. Hieraan wordt onder de AVG een apart artikel 10 gewijd. De gemeente mag o.a. strafrechtelijke gegevens verwerken in het kader van het Veiligheidshuis, zie artikel 33 lid 1 onderdeel b UAVG. Uiteraard mag dat alleen wanneer het strikt noodzakelijk is.

Ook al wordt het onder de AVG geen bijzonder persoonsgegeven genoemd, voor het burgerservicenummer (BSN) blijft gelden dat het enkel gebruikt mag worden wanneer het door de wet is voorgeschreven. Het mag ook enkel voor de doeleinden gebruikt worden die die wet bepaalt. Nederland gaat hier dus verder dan de AVG, en heeft gebruik gemaakt van de beleidsvrijheid die de AVG biedt.

Gezien het risico van het verwerken van bijzondere persoonsgegevens voor betrokkenen, zal de gemeente deze niet door derden laten verwerken, tenzij dat er zwaarwegende belangen zijn. Dit ter beslissing aan de FG. Indien desondanks bijzondere persoonsgegevens niet 'in house' worden gedraaid (maar bij een verwerker), dient het beschermingsniveau gegarandeerd te zijn. Dit betekent dat bijzondere persoonsgegevens in beginsel binnen de Europese Economische Ruimte (EER = EU + Noorwegen, IJsland, Liechtenstein) gehost dienen te worden. De FG zal hier op toezien.

9.2 Gevoelige persoonsgegevens
Onder gevoelige persoonsgegevens worden ten eerste de bijzondere persoonsgegevens gerekend. Daarnaast behoren financiële persoonsgegevens tot de gevoelige gegevens (bijvoorbeeld informatie over schulden, salarisstroken, etc). daarnaast ook persoonsgegevens op grond waarvan mensen kunnen worden 'nagewezen' (stigmatisering), zoals een goksverslaving. Tenslotte worden wachtwoorden, inloggegevens, burgerservicenummers, kopieën van identiteitsbewijzen, en bankrekeningnummers tot de gevoelige gegevens gerekend. Indien iemand ten onrechte toegang krijgt tot deze gegevens, kan daarmee (identiteits)fraude gepleegd worden[3].
Van belang is op te merken dat ook al zou iemand vinden dat het niet erg is als een gevoelig persoonsgegeven bekend wordt ('ze mogen alles van me weten') niet relevant is bij de beoordeling of een persoonsgegeven gevoelig is.
Of een persoonsgegeven gevoelig van aard is speelt onder andere een rol bij de bepaling of de gemeente persoonsgegevens die voor een bepaald doel zijn verzameld ook mag verwerken voor een ander doel. Hoe gevoeliger het persoonsgegeven, hoe minder snel de gemeente mag aannemen dat er sprake is van een verenigbaar doel.

10. Bewaartermijnen
De AVG gaat ook uit van opslagbeperking. Dit houdt in dat persoonsgegevens niet langer mogen worden bewaard dan noodzakelijkheid is voor de verwerking. Hierop moeten de zaaksystemen, afdelings- en persoonlijke schijven met opslagruimte en andere gebruikte applicaties worden gecheckt. De AVG verlangt dat de gemeente concrete termijnen benoemt, maar noemt zelf geen termijnen. Ze moeten in ieder geval een duidelijk vast te stellen einde hebben. De gemeente neemt in het verwerkingsregister de wettelijke bewaartermijnen van de verschillende verwerkingen op en stelt deze vast voor zover dat is toegestaan en nog niet gebeurd is.

11. Privacy by design en privacy by default
Privacybescherming bestaat niet alleen uit toetsen en controle achteraf. Om de zes principes van privacybescherming zoals verwoord in punt 1.2, zo goed mogelijk door te voeren, dient juist ook aan de voorkant van het ontwerpen en inrichten van processen en systemen privacybescherming als uitgangspunt genomen te worden. Voor de AVG zijn privacy by design en privacy by default belangrijke onderdelen van de verantwoordingsplicht van de gemeente.
3https:// autoriteitpersoonsgegevens.n1/sites/default/files/atoms/files/guidelines_meldplicht_datalek ken.pdf

11.1 Privacy by design
Privacy by design houdt in dat er al bij het ontwerpen van producten en diensten voor gezorgd wordt dat persoonsgegevens goed worden beschermd.

3) https:// autoriteitpersoonsgegevens.n1/sites/default/files/atoms/files/guidelines_meldplicht_datalek ken.pdf

Bij de inrichting van een proces of systeem wordt gekeken naar de eisen die vanuit de invalshoek van privacybescherming gesteld kunnen worden. Dataminimalisatie is bijvoorbeeld één van de uitgangspunten die hierbij gehanteerd worden: zo min mogelijk persoonsgegevens verzamelen, alleen datgene wat strikt noodzakelijk is voor het bereiken van het doel. Ook kunnen privacy verhogende maatregelen worden meegenomen, bijvoorbeeld door gevoelige gegevens in een afgesloten bestand te bewaren.

Voorbeelden van privacy by design: het op eenvoudige wijze kunnen uitdraaien van alle persoonsgegevens van een betrokkene die in een applicatie voorkomen, wanneer de betrokkene daar om vraagt. Ook kan de mogelijkheid worden ingebouwd dat persoonsgegevens na verloop van een bepaalde periode automatisch verwijderd worden, of in ieder geval het systeem laten waarschuwen dat de bewaartermijn verstreken is. Verder kan er aan de poort voor gezorgd worden dat de instellingen van systemen waarbij gevoelige persoonsgegevens worden verwerkt zodanig zijn dat de optie 'benaderbaar voor alle medewerkers' ontbreekt. Het proces dient zodanig te worden aangepast zodat een ID alleen getoond hoeft te worden, zodat voorkomen wordt dat een kopie van het ID onnodig wordt bewaard.

Om privacy by design te borgen in de organisatie zullen medewerkers worden getraind in het consequent toepassen van privacy by design. Daarnaast zal actief geadviseerd worden door de privacybeheerder, de CISO en de afdeling ICT over de invulling van privacy by design en zal de FG toetsen op de (tussentijdse) resultaten. Dit proces dient in komende jaren nader te worden uitgewerkt en beproefd.

11.2 Privacy by default
Privacy by default houdt in dat de gemeente technische en organisatorische maatregelen moet nemen om ervoor te zorgen dat, als standaard, alléén persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat moet worden bereikt. Bijvoorbeeld:
een app zo instellen dat de locatie van gebruikers niet onnodig wordt geregistreerd; persoonsgegevens niet met collega's delen wanneer daarvoor geen noodzaak is.
De uitwerking van deze werkwijze wordt meegenomen in het nog te ontwikkelen proces voor privacy by default.

12. Data Protection Impact Assessment
Een Data Protection Impact Assessment (DPIA) is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaartte brengen. Uitgangspunt bij een DPIA is dat afhankelijk van de verwerking passende waarborgen worden ingebouwd (Privacy by design). De DPIA legt in de eerste plaats de risico's bloot van projecten waarbinnen wordt gewerkt met persoonsgegevens, en het draagt bij aan het vermijden of verminderen van deze privacy risico's. Op basis van de antwoorden die worden gegeven in de DPIA wordt op systematische wijze inzichtelijk gemaakt of er een kans is dat de privacy van de betrokkene wordt geschaad, hoe groot deze kans is en op welke gebieden dit speelt. De DPIA doet dit op een gestructureerde wijze. Zie bijlage 4.
De AP heeft een lijst gepubliceerd met verwerkingen waarvoor het verplicht is om vooraf een PIA uit te voeren.[4] De AP adviseert voor bestaande verwerkingen die aan de genoemde criteria voldoen eens per 3 jaar een DPIA te doen. Besloten is om voor de BLNP-gemeenten 4 jaar aan te houden, gezien de hieraan verbonden kosten.

13. Anomisering/pseudonimisering

13.1 Anonimisering
Wanneer gegevens niet meer herleidbaar zijn tot natuurlijke personen, zijn ze anoniem. De AVG is dan niet van toepassing. In veel gevallen is het niet nodig om te werken met persoonsgegevens, om toch het gestelde doel te bereiken. Indien de gemeente bijvoorbeeld de gemiddelde leeftijd van een bezoeker van een gemeentelijk gebouw zou willen weten, is het niet nodig om de gegevens van alle individuele bezoekers in een bestand te zetten.
Beter is dan om alle gegevens 'weg te gooien' behalve de leeftijd. Nu zijn de gegevens niet meer te herleiden tot personen.

13.2 Pseudonimisering
Bij pseudonimiseren-van persoonsgegeven wordt, in tegenstelling tot bij anonimisering, de 'sleutel' niet weggegooid. Persoonsgegevens worden losgekoppeld van de andere gegevens en vervangen door bijvoorbeeld een code. Zolang de mogelijkheid blijft bestaan dat de codes terugvertaald worden naar persoonsgegevens, blijft de AVG van toepassing.

Pseudonimisering betekent niet dat er geen sprake meer is van persoonsgegevens. Wel is het zo dat eerder zal worden voldaan aan de vereisten van beveiliging en dat de risico's voor betrokkenen minder groot kunnen zijn (omdat herleiding veel minder makkelijk is) Pseudonimisering vereist het nemen van

4) https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia

zorgvuldige technische en organisatorische maatregelen om te kunnen waarborgen dat koppeling aan natuurlijke personen niet alsnog nodig is. De gemeente moet nog een protocol voor anonimiseren en pseudonimiseren ontwikkelen ten behoeve van passende beveiliging van persoonsgegevens.

14. Big data/tracking

14.1 Big data/ tracking
Bij Big data gaat het om het verzamelen en hanteren van zeer grote hoeveelheden data. Data gegenereerd uit elektronische activiteiten van gebruikers, en uit onderlinge communicatie tussen apparaten (machine to machine). Big-data-analyse is het gebruik van technieken, technologieën en softwaretools voor analyse van Big data uit de organisatie en/of uit andere gegevensbronnen. Bij tracking gaat het om het volgen van (het gedrag van) gebruik van gebruikers van mobiele telefoon via een wifi-verbinding, of van het surfgedrag op internet. De gemeente maakt tot op heden geen gebruik van tracking. Ontwikkelingen in het kader van o.a. Smart Cityprojecten vragen van de gemeente steeds meer toe te werken naar het gebruik van nieuwe technologieën zoals Big data en tracking. Deze technologieën kunnen nodig zijn voor het optimaal uitvoeren van bepaalde taken van de gemeente.

Een veelgehoord voorbeeld is het opslaan van gegevens over de aanwezigheid van mobiele telefoons om grote stromen (burger)verkeer te monitoren in het kader van de veiligheid van burgers tijdens, bijvoorbeeld, een nationale feestdag. Maar Big data kunnen bijvoorbeeld ook de dienstverlening verbeteren. Het gebruik van Big data en tracking mag niet leiden tot schending van de privacy. Uitgangspunt van deze gegevensverwerking is dat zo min mogelijk (persoons)gegevens worden opgeslagen en deze gegevens geanonimiseerd worden. Als dit niet mogelijk is worden de gegevens gepseudonimiseerd. Dat betekent dat we persoonsgegevens omzetten in iets wat niet meer direct herleidbaar is tot een persoon. Voor Big Data en tracking wordt door de gemeente een aantal uitgangspunten geformuleerd die het mogelijk moeten maken om met Big Data en tracking aan de slag te gaan, zonder daarbij de kaders die de privacywetgeving stelt, te overtreden.

II. DE AVG EN ANDERE WETTEN
In deze paragraaf wordt de relatie tussen de AVG en andere wetten kort behandeld. Over het algemeen geldt de AVG als een algemene wet, waarvan de bepalingen niet van toepassing kunnen zijn wanneer er bijzondere wetgeving van toepassing is.

1. AVG versus Wet Basisregistratie personen
De AVG is niet van toepassing op de WetBRP. Dit blijkt uit artikel 2 UAVG. De wet BRP geeft zelfstandig uitvoering aan de AVG.

2. AVG versus Wet politiegegevens
De AVG is niet van toepassing op de Wet politiegegevens. Dit blijkt uit artikel 2 UAVG. De de Wet politiegegevens heeft een eigen privacy regime

3. AVG versus WOB
In de AVG staat dat een verwerking van persoonsgegevens mag indien dit noodzakelijk is voor de nakoming van een wettelijke verplichting of een goede invulling van een publiekrechtelijke taak. De gemeente moet hierbij wel nagaan of het doel ook via minder ingrijpende middelen kan worden bereikt en of de verwerking noodzakelijk is. Gemeenten moeten dus van geval tot geval een belangenafweging maken of publicatie van persoons gegevens écht noodzakelijk is. In de regel zal de vermelding van de persoonsgegevens in de openbare stukken niet noodzakelijk zijn voor een goede vervulling door gemeenten van hun actieve publicatie verplichting op grond van de Gemeentewet of de Wob.

4. AVG versus Archiefwet
De AVG kent een aantal specifieke uitzonderingen voor verwerking van persoonsgegevens met het oog op archivering in het algemeen belang. Een aantal uitzonderingen werkt rechtstreeks, zie artikel 89 AVG. Artikel 89 lid 3 AVG bevat een specifieke bepaling op grond waarvan de lidstaten kunnen afwijken van enkele voorschriften van de AVG. Zie ook artikel 45 van de UAVG.

Bij verwerkingen onder de kop van onderzoek en archivering dienen de rechten van betrokkenen te worden gewaarborgd. Het accent hierbij ligt bij het beginsel van gegevensminimalisering (dataminimalisatie). Zodra het mogelijk is om het archiveringsdoel te halen met ontkoppelde gegevens (ofwel geanonimiseerde gegevens, niet langer herleidbaar tot een natuurlijke persoon en daarmee niet langer persoonsgegevens) moet deze ontkoppeling worden uitgevoerd. Als tussenvorm mag gewerkt worden met pseudonimisering waarbij koppeling nog wel mogelijk is, maar de daarvoor benodigde informatie niet direct beschikbaar is.

De gemeente dient kritisch te kijken binnen de eigen werkprocessen voorafgaand aan archivering en deze te toetsen op dataminimalisatie, zodat kan worden aangetoond dat ook voor wat betreft het ge-

meentelijke archief voldaan is aan de vereiste passende waarborgen die voortkomen uit de AVG en de UAVG.

5. AVG versus identiteitsbewijs
In veel gevallen is een burger verplicht zich te identificeren met een geldig identiteitsbewijs (de Wet Identificatieplicht en bijzondere wetten). Dat betekent niet per se dat dan ook een kopie daarvan bewaard mag worden. Een identiteitsbewijs bevat een burgerservicenummer en kan bijzondere persoonsgegevens bevatten (ras). Verwerken is dus verboden tenzij. Een voorbeeld: de wet op de loonbelasting verplicht de gemeente als werkgever een kopie van een identiteitsbewijs van een ambtenaar/werknemer tot 5 jaar te bewaren na het jaar waarin deze persoon uit dienst is getreden. Hier is dus een wettelijke grondslag voor het bewaren van een kopie van een identiteitsbewijs.

Bijlage 3 bij privacybeleid 2020 van de gemeenten Bunschoten, Leusden, Nijkerk en Putten

Incident management en respons
Een incident is een gebeurtenis die een gevaar vormt voor de kwaliteit van de gemeentelijke informatiebeveiliging. Een informatiebeveiligingsincident is elke onverwachte of onverhoopte gebeurtenis die de informatiebeveiliging van een organisatie kan aantasten. Hieronder kan vallen:

- Diefstal;
- Bedreiging of intimidatie;
- Fraude;
- Uitlekken van gevoelige informatie;
- Inbreuken;
- Verlies van gegevens en documenten;
- Fouten in het netwerk, applicaties of berichtenverkeer;
- Fouten veroorzaakt door mensen;
- Verstoring van de bedrijfsvoering.

Incident management is belangrijk, omdat 100 procent beveiligen niet bestaat en incidenten niet helemaal te voorkomen zijn. Het is belangrijk om ingericht te hebben hoe te handelen wanneer er sprake is van (het vermoeden van) een incident om zo de schade zo snel mogelijk te beperken en het probleem op te lossen.

Hiervoor is een beleid, het incident management en response beleid, opgesteld. Daarnaast bevat dit document een procedure om op een juiste manier om te gaan met informatiebeveiligingsincidenten. Hiermee wordt tegemoetgekomen aan doelstelling 13 van de Baseline Informatiebeveiliging voor Nederlandse Gemeenten (BIG). Het geeft de gemeente richting aan de wijze waarop de gemeente wenst om te gaan met alle incidenten en bijna incidenten op het gebied van informatiebeveiliging. De uitgangspunten van dit document zijn:

- Het beleid is van toepassing op iedereen die werkzaam is bij de gemeente.
- iedereen die werkzaam is binnen de gemeentelijke organisatie is verplicht om waar nodig gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht.
- iedereen die werkzaam is binnen de gemeentelijke organisatie is verplicht om van (vermeende) inbreuken, die in verband staan met het bovenstaande, melding te maken.
- Waar mogelijk wordt gebruikgemaakt van de kennis die aanwezig is binnen de samenwerking Bunschoten, Leusden, Nijkerk en Putten (BLNP).

Incident management en response beleid
Om richting te geven aan de wijze waarop de gemeente wenst om te gaan met alle (bijna) incidenten op het gebied van informatiebeveiliging is dit beleid opgesteld. Dit beleid is opgesteld met als uitgangspunten het informatiebeveiligingsbeleid 2015, de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG), die in 2019 vervangen wordt door de BIO (Baseline Informatiebeveiliging Overheid) en de Algemene Verordening Gegevensbescherming (AVG), die sinds 25 mei 2018 van toepassing is.

1. Informatiebeveiligingsgebeurtenissen en zwakheden die verband houden met informatiesystemen worden zodanig kenbaar gemaakt dat de gemeente tijdig en adequaat corrigerende maatregelen kan nemen. Dit omvat ook het regelmatig beoordelen van loggegevens van informatiesystemen.
2. Informatiebeveiligingsgebeurtenissen moeten zo snel als mogelijk via de leidinggevende, de helpdesk of de CISO (Chief Information Security Officer) gerapporteerd worden.
3. Alle werknemers, ingehuurd personeel en externe gebruikers van gemeentelijke informatiesystemen en diensten moeten alle waargenomen of verdachte zwakke plekken melden volgens de procedure. Dit geldt ook voor geconstateerde of vermoede beveiligingslekken en beveiligingsincidenten.
4. Informatiebeveiligingsincidenten moeten vastgelegd en beheerd worden en hiervoor is een procedure gemaakt. Deze procedure moet bekend zijn bij alle werknemers. In deze procedure moet de verantwoordelijkheden belegd worden.
5. Wanneer het om een incident gaat waarbij er sprake is van een inbreuk op de persoonsgegevens, wordt afhankelijk van de ernst hiervan" op grond van artikel 33 AVG een melding gedaan bij de Autoriteit Persoonsgegevens (AP) en wanneer dat noodzakelijk is op grond van artikel 34 AVG (waarschijnlijk een hoog risico voor de rechten en vrijheden van natuurlijke personen), wordt de inbreuk gemeld aan de betrokkene(n).
6. Incidenten worden wanneer noodzakelijk gemeld bij de informatiebeveiligingsdienst (IBD), zodat advies ingewonnen kan worden en dat er een waarschuwing uit kan gaan naar andere gemeenten.
7. Informatiebeveiligingsmeldingen moeten periodiek beoordeeld worden met als doel de beheersmaatregelen te verbeteren.

8. Informatiebeveiligingsincidenten kennen soms een vervolgprocedure, daarom moet zoveel als mogelijk bewijsmateriaal verzameld worden in overeenstemming met de voorschriften.
9. Informatiebeveiligingsincidenten moeten geëvalueerd worden, zodat de procedure kan worden bijgesteld en beheersmaatregelen kunnen worden verbeterd.
10. Ernstige incidenten waarbij een alarmfase in werking treedt, zoals weergegeven is in het informatiebeveiligingsbeleid, worden opgenomen in de kwartaalrapportage van de CISO.
11. Bij grote incidenten wordt gehandeld en opgeschaald conform de draaiboeken ICT crisisbeheersing.

Incident Response Team
Voor de interne crisisbeheersing is een kernteam samengesteld, dat samenkomt in het geval van grote incidenten en calamiteiten. Hieronder vallen onder andere de datalekken. In het onderstaand overzicht is weergegeven welke functies vast onderdeel zijn van het kernteam en welke rol zij daarin vervullen.

CISO	Voorzitter/initiator,adviseur (welke rollen?)
Regionale CISO	Wanneer het een incident betreft dat meerdere gemeenten in **BLNP** raakt wordt de regionale CISO-onderdeel van het kernteam
Functionaris Gegevensbescherming	Neemt uitsluitend deel wanneer het een incident betreft in één of meer van de BLNP-gemeenten waarbij er sprake is van een inbreuk op de persoonsgegevens
Gemeentesecretaris of vervanger	Besluitvormer (deze kan ook alleen geïnformeerd worden om een besluit te kunnen nemen)
Privacybeheerder	Adviseur, neemt uitsluitend deel wanneer het een incident betreft in de lokale gemeente of in één of meer BLNP-gemeenten voor wie de privacybeheerder taken waarneemt
Beveiligingsbeheerder ICT	Adviseuren/of uitvoerende aangaande ICT componenten van het incident.

Overige betrokkenen
Naast het kernteam kunnen er nog andere personen betrokken worden bij de afhandeling van een incident, omdat zij vanuit hun expertise een goede bijdrage kunnen leveren of omdat zij tijdig ingeschakeld dienen te worden in verband met een toezichthoudende rol. Hierbij gaat het om specialisten die over bepaalde kennis beschikken om tot een goed besluit en een efficiënte afronding te komen, danwel de toezichthoudende instantie.

Controller informatiebeveiliqinq	Controleur en wanneer nodiq adviseur
Beleidsmedewerker communicatie	Adviseur en/of uitvoerende aangaande de communicatie rondom het incident.
Juridisch controller	Adviseurover de juridische aspecten van het incident.
Afdelingsmanager van de afdeling waarhet incident heeft plaatsqevonden	Uitvoerende/delegerende
Externe deskundige, Autoriteit Persoonsgegevens, bureau met bepaalde expertise	Advies, Toezicht

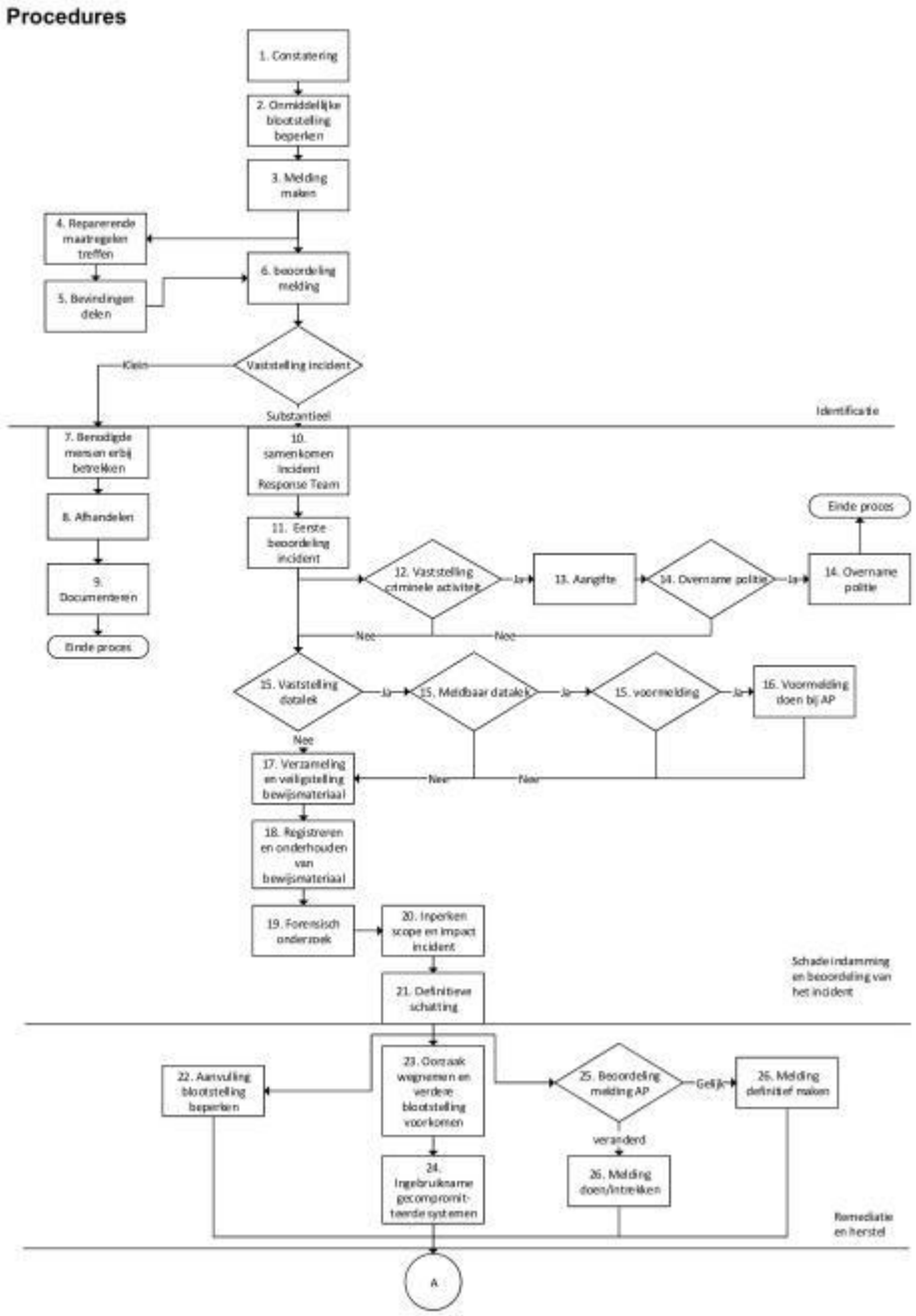
Incident management response procedure
Voor een succesvolle reactie op incidenten dienen een aantal stappen doorlopen te worden, welke in samenhang het incident management response proces genoemd worden. Het is belangrijk dat op een gestandaardiseerde wijze melding gemaakt wordt van vermeende incidenten en dat deze op een gestructureerde manier afgehandeld worden.

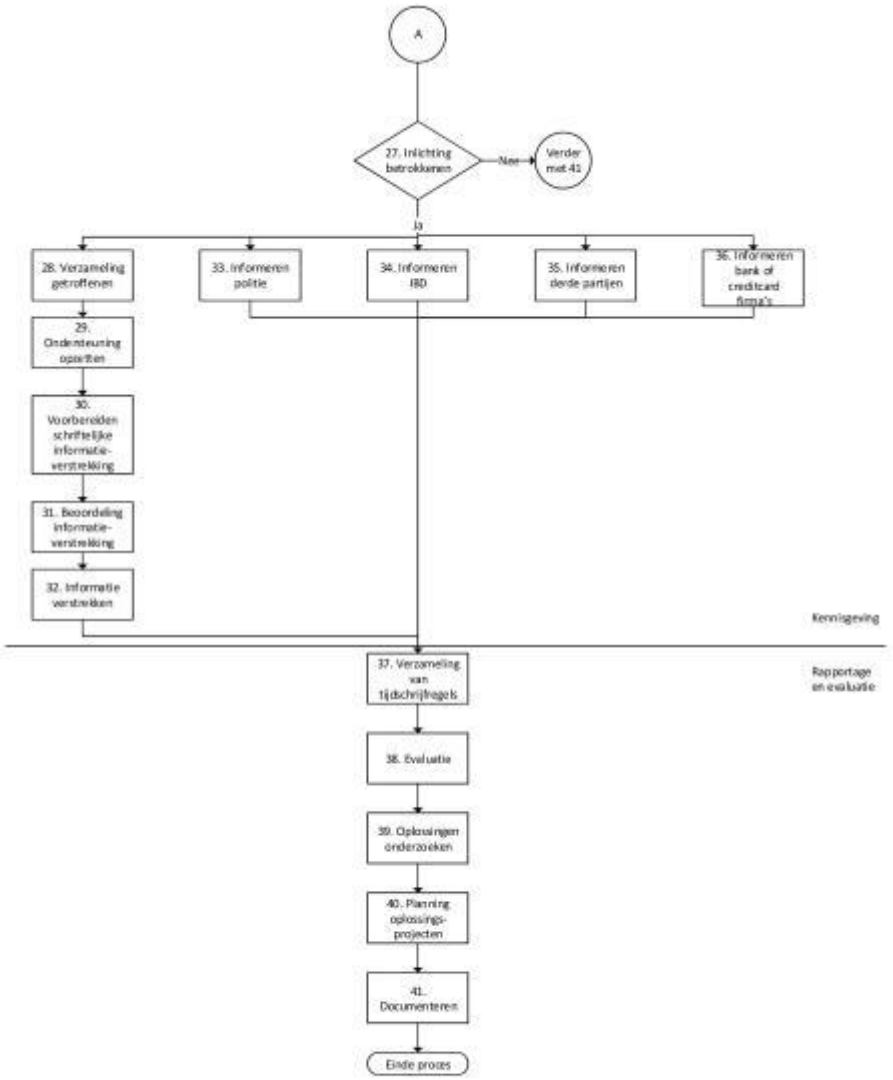
Hiervoor is het proces beschreven in het document voorbeeld incident management en responsebeleid van de informatiebeveiligingsdienst voor gemeenten gebruikt als input. Dit proces bestaat uit een aantal stappen, te weten:
1. Identificatie.
   Deze stap omvat de controle of het incident daadwerkelijk plaatsgevonden heeft.
2. Schade indamming
   Bij deze stap wordt een start gemaakt met het oplossen van het incident.
3. Remediatie en herstel

Bij deze stap wordt invoering gegeven aan de oplossing van het incident en wordt een start gemaakt met het herstel.

4. Kennisgeving
   Deze stap omvat het in kennis stellen van betrokkenen en andere overheidsinstanties.
5. Rapportage en evaluatie
   Deze stap omvat de lering die getrokken kan worden uit het incident en de vervolgstappen die daaruit voortkomen.

Procedures





Nr.	Functionaris*	Activiteit	Omschrijving
1	MW,AD,AM, SB, andere instantie	Constatering	Een medewerker, systeembeheer of een andere instantie constateert dat er een zwakke plek, een beveiligingslek of een beveiliqinqsincident (moqeliik) heeft plaatsgevonden.
2	MW,AD,AM	Onmiddellijk blootstelling beperken	Als een elektronisch apparaat is gecompromitteerd: • Niet gebruiken (nietinloggen) of wijzigen van het apparaat • Zet het apparaat niet uit • Haal de netwerkverbindingen er af, maar NIET de voedingskabel Noteer hoe het incident werd ontdekt en welke acties er tot nu toe genomen zijn. Geef een zo specifiek mogelijk antwoord, inclusief data, tijden, en welke apparaten gecompromitteerd zijn, applicaties, websites, et cetera
3	MW,AD,AM CISO BLNP CISO FG	Melding van het incident	Waarschuw onmiddellijk: • De lokale CISO

	PB		• De lokaleCISO meldt bij (vermoeden van) inbreuken i.v.m. persoonsgegevens: BLNP CISO en FG en lokale PB • Het management/gemeentesecretaris De controller/informatiebeveiliger BRP en Reisdocumenten wanneer sprake is vanincidenten met persoonsgegevens vanuit BRP. Dit kan gedaan worden door de melding door te geven aan de helpdesk ICT, die vervolgensde CISO waarschuwt. Deze licht de andere personen in. Het is ook mogelijk om een directe melding te doen naar de afdelingsmanager, de CISO of controller. Degene die ingelicht wordt, meldt dit aan de ander. Ook wordt de archivaris geïnformeerd, zodat het meegenomen kan worden bij de verantwoording.
4	HD, SB	Reparerende maatregelen treffen	Naast de maatregelen die de afdeling getroffen heeft kan het zijn dat er extra reparerende maatregelen getroffen moeten worden om de blootstelling te beperken dan wel weg te nemen.
5	HD, SD	Bevindingen delen	Helpdesk en systeembeheer deelt de informatie die zij te weten gekomen zijn tijdens het treffen van de reparerende maatregelen metde CISO zodat vastgesteld kan worden of het incident daadwerkelijk plaatsgevonden heeft en deze informatie is input voor de verdere afhandeling van het proces.
6	CISO, SB FG PB	Beoordeling melding	Bij deze stap wordt gekeken of het incident daadwerkelijk plaatsgevonden heeft. Wanneer het een digitaal incident betreft wordt systeembeheer bij deze stap betrokken. Ook wordt er een second opinion gevraagd aan de collega CISO's binnen BLNP. Hierbij wordt een voorlopige beoordeling gemaakt van de type en de scope van het incident en de omvang van de blootstelling en wordt een prioritering gegeven.

			Hierbij moet gebruikgemaakt worden van leidraad prioritering incidenten in het voorbeelddocument incident management en responsebeleid van de IBD. Er wordt een start gemaakt met een logboek waarin alle activiteiten op datum en wanneer nodig tijd worden vastgelegd. Daarnaast moeten mogelijk de volgende personen/groepen op de hoogte gehouden worden: • College van B en W • Gemeentesecretaris • Het management • Communicatie/Voorlichting • De controller/informatiebeveiliger BRP en Reisdocumenten wanneer het om persoonsgegevens gaat vanuit het BRP.
7	CISO	Benodigde mensen erbij betrekken	De CISO brengt in deze stap de mensen samen die het incident gezamenlijk gaan afhandelen. Deze mensen worden in deze stap geïnformeerd over de situatie voor zover zij nog niet bekend zijn met het incident en er wordt een taakverdeling gemaakt voor de afhandeling van het incident.
8	HD, SB, AD, AM	Afhandeling	Op basis van de taakverdeling wordt het incident verholpen en afgehandeld. De CISO houdt een logboek bij van de taken die zijn uitgevoerd en de keuzes die gemaakt zijn.
9	CISO, SB	Documenteren	Het incident wordt te allen tijde gedocumenteerd in het incidentenregister ongeacht of het gaat om een inbreuk op de persoonsgegevens of niet. 2.
10	CISO	Samenkomen Incident Response Team	In deze stap wordt het team dat samengesteld is bij elkaar geroepen. De groep kan per incident aangevuld worden met andere expertises die nog niet standaard in het team vertegenwoordigd zijn. Dit team gaat samen de rest van het proces uitvoeren. Bij deze stap wordt het huidige proces beoordeeld en worden de verantwoordelijkheden besproken en toebedeeld. Bij de uitvoering van deze activiteit zijn de volgende dingen belangrijk: - Verstrek ieder teamlid de huidige Incident Management Checklist.

			- Bespreek de communicatiestrategie. - Bespreek het belang van het goed in een tijdlijn documenteren en het voorkomen van het verloren raken van onderzoeksgegevens. In de communicatie binnen het team in deze fase, is het vooral belangrijk om nauwkeurig de feiten te tussen teamleden onderling en tussen het team en de juiste ambtenaren. *Hierbij geldt bijvoorbeeld dat:* - *Teamleden niet met anderen buiten het team mogen praten over het incident totdat de gemeentesecretaris daarvoor toestemming heeft gegeven* - *Alle documentatie die door het team geschreven wordt op feiten gebaseerd moet zijn en goed gedocumenteerd moet zijn omdat deze gegevens mogelijk in een strafrechtelijk onderzoek gebruikt kunnen worden.* - *Er geregeld overleg tussen de teamleden.*

11	IRT	Eerste beoordeling incident	Bij deze stap maakt het Incident Response Team een beoordeling van het incident. Ze stellen het volgende vast: - Of het gaatom een criminele activiteit, - Of het gaat om een datalek, of deze meldbaar is en of er een voormelding gedaan moet worden bij de Autoriteit Persoonsgegevens. - De wijze van onderzoek.
12	IRT	Beoordeling criminele activiteit	Bij deze stap wordt gekeken of het incident te maken heeft met een criminele activiteit. Wanneer dit het geval is kan er sprake zijn van een andere verloop van het proces. Dit zijn incidenten die gaan over elektronische apparaten en gestolen of verloren media, ongeacht de vorm. Dit betekent ook papier etc.
13	GS	Aangifte	Wanneer er sprake is van een criminele activiteit moet altijd aangifte gedaan worden bij de politie. De bepaling of aangifte gedaan moet worden gebeurd altijd in overleg met de burgemeester om de noodzakelijke acties en stappen te bepalen. Het lekken van informatie met betrekking tot personen zal conform de wetgeving gemeld moeten worden.
14	AD, CISO	Overname politie	Wanneer aangifte gedaan wordt bij de politie moet bepaald worden op de politie het onderzoek over moet nemen. Wanneer dit het geval is moet dit gedocumenteerd worden. Wanneer dit niet het geval is wordt het proces verder doorlopen. De documentatie wordt gedaan door de betreffende afdeling in samenwerking met de CISO
15	IRT FG PB	Vaststellen datalek en afwegen of dit gemeld moet wordenbij de AP enbij de betrokkene(n)	In deze beslissingsstap beoordeelt de FG, na overleg met de leden van het Incident Response Team of het incident een datalek betreft dat op grond van artikel 33 AVG (al of niet voorlopig) binnen 72 uur gemeld dient te worden aan de Autoriteit Persoonsgegevens (AP). Een voorlopige melding kan later weer worden ingetrokken. - Ook beoordeelt de FG, na overleg met het IRT, proceseigenaren of andere intern betrokkenen (b.v. juridisch adviseurs) of dit incident ook vanwege een hoog risico voor rechten en vrijheden van de betrokkene(n), op grond van artikel 34 AVG gemeld dient te worden aan de betrokkene(n) en anderen (b.v. overige inwoners van de gemeente). - De FG is bevoeqd om daarbij zo nodiq inlichtingen en advies over de afhandeling van het incident in te winnen bij de Informatiebeveiligingsdienst Gemeenten (IBD) of andere externe instanties. - De FG adviseert vervolgens de verwerkingsverantwoordelijke over de afhandeling van het datalek... - Dit advies wordt binnen de BLNP-gemeenten -uit praktische overwegingen- doorgaans via de privacybeheerder kenbaar gemaakt aan de meest verantwoordelijke proceseigenaar en aan de gemeen-

			tesecretaris. De uiteindelijke beslissing of er wel of geen melding gemaakt wordt bij de AP ligt bij de gemeentesecretaris en bij diens afwezigheid bij de loco- secretaris. - Bij ernstige incidenten zal de FG, na overleg met het de leden van het IRT, de meest verantwoordelijke proceseigenaar, de vakwethouder adviseren over het datalek en het maken van de afweging of en zo ja op welk moment de verwerkingsverantwoordelijke (meestal het college, soms de burgemeester) geïnformeerd dient te worden. Het college/de burgemeester maakt de afweging of de gemeenteraad geïnformeerd wordt.

16	PB	Melding maken bij AP en de betrokkene(n)	- Als de gemeentesecretaris instemt met melding bij de AP, geschiedt dit volgensde Meldplicht van de AP, respectievelijk de richtlijnen van de EU-groep gegevensbescherming artikel 29., zie https://autoriteitpersoonsgegevens.nVnl/onderwerpen/beveiliging/meldplicht-datalekken en https://autoriteitpersoonsgegevens.nVsites/defaulUfiles/atoms/files/guidelines meldplicht datalekken.pdf., zie met name het schema op blz 35 van deze guidelines. De FG kan -zonodig- direct escaleren naar de gemeentesecretaris indien het FG- advies niet of niet tijdig wordt opgevolgd. Dit moet gedaan worden binnen 72 uur of met motivatie waarom de melding later gedaan wordt. De PB verzorgt dan in opdracht van de gemeentesecretaris en in overleg met FG en Responseteam de melding bij de Autoriteit Persoonsgegevens (AP). Hierbij wordt het volgende gemeld: - De aard van de inbreuk. - De namen van instanties die meer informatie over de inbreuk kunnen geven. - De aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken. - Een beschrijving van de geconstateerde en de vermoedelijke gevolgen van de inbreuk voor de verwerking van persoonsgegevens. - De maatregelen die de gemeente heeft genomen of voorstelt te nemenom deze gevolgen te verhelpen.

17	IRT	Verzameling en veiligstelling bewijsmateriaal	Bij deze stap wordt fysiek en digitaal bewijs verzameld die samen een duidelijke en gedetailleerde beschrijving geven van hoe de data gecompromitteerd kon worden. Wanneer digitale sporen zeker gesteld moeten worden, wordt een externe specialist erbij gehaald om de sporen op de juiste manier te verkrijgen en geen sporen verloren te laten gaan. Hierbij wordt aan de volgende aspecten aandacht besteed: - De aard van het incident. - Oorzaak van het incident. - Aanwezigheid van niet nakomen of een tekortkoming in informatiebeveiligingsprocedures. - De verwijtbaarheid van het incident. - Deherstelling van een tekortkoming in de beveiliging. - Herhaling van het incident. - Noodzakelijke acties om herhaling te voorkomen.
18	IRT	Registreren en onderhouden van het bewijsmateriaal	Bij deze stap worden de bewijsmaterialen geregistreerd en bijgehouden waar het bewijsmateriaal zich bevindt en wie er toegang toe heeft. Dit betekent dat er een inventarisatielijst van alle bewijsmateriaalgemaakt moet worden waarop bijgehouden wordt wie, wanneer en watgedaan heeft met het bewijsmateriaal. Een richtlijn hiervoor is: 1. Geef een exacte beschrijving van het bewijsmateriaal. 2. Leg vast wie erbijmoest en waarom. 3. Leg vast waar en op welke wijze het bewijsmateriaal opgeslagen is. 4. Als apparatuur verplaatst moet worden zorg dan dat de ontvanger weet welke verantwoordelijkheden er zijn, dat de ontvanger tekent

			voor ontvangst en dat dit bewijs wordt toegevoegd aan de verzameling.
19	IRT	Forensische onderzoek	Bij deze stap wordt de volgende taken uitgevoerd en vastgelegd: 1. Analyseren van bewijsmateriaal. 2. Het uitvoeren van eenreconstructie van het incident. 3. Het zorgen voor gedetailleerde documentatie. Hierbij wordt het originele bewijsmateriaal bewaart en alleen gewerkt met een kopie van de data. Er wordt gezorgd voor een zo minimaal mogelijke verstoring van de bedrijfsvoering en voor herleidbare en herhaalbare resultaten. In geval van digitaal bewijsmateriaal wordt een externe specialist gecontacteerd.

20	IRT	Inperken scope en impact van incident	Tijdens deze stap worden er maatregelen genomen om de reikwijdte en de impact van het incident in te perken.
21	IRT	Definitieve schatting	Maak de definitieve schatting af, en de documentatie over soort en afbakening van de blootgestelde data, evenals de beschikbaarheid en het soortvan contactinformatie van de betrokken personen.
22	IRT	Aanvulling blootstelling beperken	Dit is een aanvulling op stap 16. Het gaat het team op zoek naar aanvullende manieren om blootstelling te beperken
23	IRT	Oorzaak blokkeren of verwijderen en verdere blootstelling voorkomen	Bij deze activiteit worden de kwetsbaarheden van systemen verwijderd of verminderd, worden toegangsrechtenen risico's bij remediatie van medium voor gevoelige dataopslag beoordeeld.
24	IRT	Weer ingebruikname gecompromitteerde systemen	Als het onderzoek naar de bewijslast op de gecompromitteerde systemen klaar is kunnen ze weer in gebruik genomen worden.
25	IRT	Beoordeling melding aan AP	In deze stap wordt beoordeeld of de eerdere melding bij de AP nog gerechtvaardigd is, of dat uit onderzoek gebleken is dat het niet een datalek betreft, dan wel één die niet gemeld hoeft te worden bij de AP.
26	PB	Melding definitief maken/Melding doen/ Melding intrekken	Op basis van de beslissing uit de vorige stap wordt er alsnog melding gedaan, wordt de melding door de PB definitief gemaakt of ingetrokken. Hiervan wordt documentatie bewaard.
27	IRT	Beoordeling inlichting betrokkenen	In deze stap wordt bepaald of het noodzakelijk is om betrokkenen te informeren. Hierbij wordt wanneer nodig gebruikgemaakt van de beleidsregels die opgesteld zijn door de AP. Daarnaast worden de volgende vragen gesteld: - Geeft de mate van risico blootstelling de noodzaak tot het informeren van getroffenen? - Zoja, o Indien van toepassing, is het de taak van rechtshandhaving om de betrokken partijen te infomeren? o Wie gaat het schrijven uitgeven? o Wie zal zich bezighouden met het beantwoorden van telefoon en e-mail op vragen van de betrokken personen? Rechtvaardigt het verwachte volume het opzetten of inzetten van een callcenter? o Is het noodzakelijk om een officieel persbericht te plaatsen op de website van de gemeente? Bij de uitvoering van deze stap kunnen de volgende richtlijnen gebruikt worden: - beslissingen die genomen moeten worden dienen in overeenstemming te zijn met eerdere beslissingen, tenzij eventuele afwijkingen volledig gerechtvaardigd zijn. Voor alle beslissingen moeten de afzonderlijke wetten, regelgeving en contractuele verplichtingen gevolgd worden.

			- Er dient een geschikt communicatiemiddel gekozen worden, passend bij het incident, de hoeveelheid te informeren personen, de mate waarin risico gelopen is en /of informatie gecompromitteerd is. - Er dient juridisch advies ingewonnen te worden over de positie en aansprakelijkheid van de gemeente bij bepaalde communicatie.

28	AD, geadviseerd door CISO/IRT	Verzameling getroffenen	Tijdens deze stap worden de naam- en adresgegevens van de getroffenen verzameld. Hierbij moet gezorgd worden dat de verzamelde data veilig wordt behandeld, verstuurd en opgeslagen. Ook is het belangrijk dat de data vernietigd wordt wanneer deze niet langer nodig is.
29	AD, geadviseerd door CISO/IRT	Ondersteuning	Het is belangrijk telefoon- en emailondersteuning op te zetten in het geval van vragen. Hiervoor moet het volgende gedaan worden: - Stel een team samen. - Zorg voor voldoende infrastructuur, beoordeel of de lijn en e-mail capaciteit voldoende is. - Kies een geschikt telefoonnummer om te gebruiken. - Kies een geschikt e-mailadres om te gebruiken. - Bedenk van tevoren de reacties op de verwachte vragen. - Train het team.
30	**AD ,** geadviseerd door IRT	Voorbereiding schriftelijke informatieverstrekking	Deze stapomvat het bedenken van het onderwerp, het toepassen van de huisstijl en het schrijven van de concepttekst.
31	PB	Beoordeling informatieverstrekking	Nadat de concepttekst van de informatieverstrekking door de afdeling afgerond is doen de privacybeheerder en communicatie een check op de tekst of deze verstrekking juist is.
32	AD, geadviseerd door IRT	Informatie verstrekken	Nadat de voorbereiding en de check afgerond is, kan de informatie verstrekt worden aan de getroffenen.
33	GS	Informeren van de politie	Wanneer het noodzakelijk of verplicht is moet de politie ingelicht worden en alsnog aangifte gedaan worden wanneer dit in het begin van het proces nog niet gedaan is.
34	/ACIB/ VCIB	Informeren van de IBD	Ook de Informatie Beveiligingsdienst (IBD) moetgeïnformeerd worden.
35	AD	Informeren van derde partijen	Wanneer met het informeren van bijvoorbeeld serviceproviders het risico van identiteitsdiefstal verkleind kan worden of als het is vastgelegd in het afzonderlijke contract moeten derde partijen geïnformeerd worden.

36	IRT	Informeer bankof creditcard firma's	Deze stap wordt uitgevoerd wanneer bankgegevens blootgesteld zijn aan niet rechthebbenden.
37	IRT	Verzameling van tijdschrijfregels	Iedereen die heeft meegewerkt aan de Incident Response- actie en tijd geschreven heeft rapporteert aan het management. De totale kosten kunnen mogelijk van belang zijn wanneer er een rechtszaak komt tegen een verdachte, omdat deze verhaald kunnen worden.
38	IRT	Evaluatie	Planeen vergadering om een evaluatie uit te voeren over de aanpak van het incident. Deze vergadering dient ongeveer twee tot zes weken na het incident plaats te vinden.

39	IRT	Onderzoek oplossingen	Onderzoek oplossingen om herhaling van het incident te voorkomen en rapporteer hierover indien nodig aan het management. Hierbij moeten de volgende vragen beantwoord worden: 1. Waarom was de data opgeslagen op een verkeerde plaats of niet veilige plaats? 2. Wat hadden we meer kunnen doen om de inbraak te voorkomen? 3. Neemt de afdeling voldoende maatregelen om herhaling te voorkomen?
40	AD	Planning oplossingsprojecten	Deze oplossingen kunnen geplaatst worden binnen oplossingsprojectenom de geleerde lessen effectief in te bedden in de organisatie. Hierin is ook aandach tvoor de evaluatie.
41	CISO FG PB	Opslag en vernietiging van Incident en Respons Informatie	Wanneer allevoorgaande activiteiten uitgevoerd zijn moet alle Incident en Response Informatie veilig opgeslagen worden (incl. gespreksverslagen, aantekeningen en incident artefacten). Op enig moment moet in overeenstemming met wetgeving en intern beleid (een deel van) de opgeslagen informatie vernietigd worden. Na deze stap is het proces beëindigd.

* Legenda afkortingfunctionarissen

- ACIB = algemeen contactpersoon Informatiebeveilig (IBD)
- AD= afdeling
- AM= Afdelingsmanager
- CISO= Chief Information SecurityOfficer
- GS = Gemeentesecretaris
- HD = Helpdesk
- IRT= Incident Response Team (FG, BLNP-CISO, lokale CISO's, lokale Informatiemanagers)
- FG= Functionaris voor gegevensbescherming
- MW= medewerker
- SB= systeembeheer
- VCIB = vertrouwelijk contactpersoon Informatiebeveiliging (IBD)
- PB = Privacybeheerder (lokaal)Bijlage incidentmeldingsniveau

Om de helpdesk te ondersteunen bij het herkennen van een beveiligingsincident en het inschatten van de impact, zijn de volgende tabellen opgenomen, welke gebaseerd zijn op het voorbeeld van incident en response beleid beschikbaar gesteld door de IBD. Deze tabel is niet compleet, maar geeft een inschatting van het niveau van melding. Wanneer het persoonsgegevens vanuit het BRP betreft wordt een andere weg bewandeld dan hieronder aangegeven is. Het incident wordt eerst gemeld bij de controller/informatiebeveiliger BRP en Reisdocumenten en deze persoon meldt het incident bij de benodigde personen.

GEBRUIKERSINCIDENTEN		**Impact***		
Incidenten categorie	**Mogelijk incident**	**Laag**	**Midden**	**Hoog**
Onopzettelijk foutief handelen	Als gevolgvan foutieve procedures	**X**		
	Als gevolg van foutgevoelige bediening	**X**		
	Onzorgvuldige omgang met password	**X**		
Opzettelijk foutief-handelen	Niet volgen van voorschriften	**X**	**X**	**(X)**
	Fraude of diefstal	**X**	**X**	**X**
	Ongeautoriseerde toegang door medewerker	**X**	**X**	**X**
Technischfalen van apparatuur	Storing in pc of randapparatuur	**X**		
Technisch falen van apparatuur door externe invloeden	Wegvallen elektrische spanning	**X**	**X**	

Menselijke omgang met apparatuur	Bedieningsfouten	X		
	Opzettelijke wijzigingen	X	X	(X)
	Beschadiging of vernieling	X	X	X
Problemen met programmatuur	Fouten in programmatuur	X		
	Ongeautoriseerd gebruik	X	X	
	Wijziging door medewerker	X	X	X
	Opzettelijk introduceren van een virus door medewerker	X	X	X
	Inbrengen van virus door middel van niet gescreende programmatuur	X	X	X
	Illegaal kopiëren	X	X	X
	Diefstal van programmatuur	X	X	X
Gegevens en gegevens- dragers	Zoekraken gegevensdragers	X	X	X
	Diefstal van gegevensdragers	X	X	X
	Beschadiging gegevensdragers	X		
	Onleesbaarheid van gegevensdragers	X		
	Fouten in gegevensdoor apparatuur	X		
	Fouten in gegevens door programmatuur	X		

GEBRUIKERSINCIDENTEN		**Impact***		
Incidenten categorie	**Mogelijk incident**	**Laag**	**Midden**	**Hoog**
	Opzettelijke invoer van foutieve gegevens	X	X	X
	Onopzettelijke invoer van foutieve gegevens	X		
	Illegaal kopiëren van gegevens	X	X	X
	Ongeoorloofd inzien van gegevens bijvoorbeeld bij invoer of printen	X	X	X
	Onzorgvuldige vernietiging van gegevens	X	X	X
Omstandigheden op de werkplek (Faciliteiten)	Uitval van elektriciteit	X		
	Wateroverlast door lekkage	X		
	Ongewenste trillingen	X		

BEHEERINCIDENTEN		**Impact***		
Incidenten categorie	**Mogelijk incident**	**Laag**	**Midden**	**Hoog**
Identificatie en bevoegdheden van gebruikers	Geen eenduidige gebruiker bij een user-ID geconstateerd	X	X	
	Ongeautoriseerde toegang door medewerker	X	X	X
	Er komen gebruikers voor die niet meer bevoegd zijn (ex-medewerkers)	X	X	
	Vraagtekens bij bevoegdheden van bepaalde gebruikers of beheerders	X	X	
Onopzettelijk foutief handelen van gebruikers	Onzorgvuldige omgang met wachtwoorden door gebruikers	X	X	
Opzettelijk foutief handelen van gebruikers	Kraken of omzeilen toegang door medewerkers of een buitenstaander	X	X	X
	Fraude of diefstal	X	X	X
Technischfalen van apparatuur	Storing in apparatuur	X	(X)	
Technisch falen van apparatuur door externe invloeden	Wegvallen elektrische spanning of spanningsschommelingen	X	X	X
	Wateroverlast	X	X	X

	Uitval netwerkverbinding door aanval met grote hoeveelheden data	X	X	X
Omgang met apparatuur door gebruikers of derden	Beschadiging apparatuur	X	X	X
	Diefstal van apparatuur	X	X	X
	Apparatuur blijkt nietgeregistreerd	X		
	Geregistreerde apparatuur blijkt niet aanwezig	X	X	
Onopzettelijk foutief handelen	Fouten in handleiding	X		
Problemen met programmatuur	Fouten in programmatuur	X	(X)	

BEHEERINCIDENTEN		**Impact***		
Incidenten categorie	**Mogelijk incident**	**Laag**	**Midden**	**Hoog**
	Ongeautoriseerde wijzigingen in programmatuur	X	X	
	Introductie van virussen via programmatuur	X	X	X
	(On)opzettelijk ongeautoriseerd gebruik	X	X	
	Gebruik van ongeautoriseerde programmatuur	X	X	
Gegevens en gegevensdragers	Ongeautoriseerde toegangtot gegevens	X	X	X
	Zoekraken gegevensdragers	X	X	X
	Diefstal van gegevensdragers	X	X	X
	Beschadiging gegevensdragers	X		
	Onleesbaarheid van gegevensdragers	X		
	Fouten in gegevens door apparatuur	X		
	Fouten in gegevens door programmatuur	X		
	Opzettelijke invoer van foutieve gegevens	X	X	X
	Onopzettelijke invoer van foutieve gegevens	X		
	Illegaal kopiëren van gegevens	X	X	X
	Ongeoorloofd inzien van gegevens bijvoorbeeld bij invoer of printen	X	X	X
	Onzorgvuldige vernietiging van gegevens	X	X	X
Facilitaire structuren en omgeving	Kortsluiting /stroomuitva1	X	X	X
	Wateroverlast door lekkage	X	X	X
	Ongeoorloofde toegang tot computer- ruimte	X	X	X
	Uitgifte sleutels aan ongeautoriseerde	X	X	X
Diensten van derden	Cruciale diensten worden (tijdelijk) niet of onvoldoende geleverd	X	X	
	Niet gescreend personeel		X	X
	Schending vertrouwelijkheid	X	X	X
	Misbruik van toevertrouwde middelen (gegevens, documentatie, en dergelijke)	X	X	X

* De impact geeft aan op welk niveau er mogelijk geëscaleerd moet worden.

- Laag: het incident/probleem wordt opgelost door ICT. Er wordt een melding gedaan bij de CISO.
- Midden: het incident/probleem wordt in beginsel opgelost door ICT. Er wordt een melding gedaan bij de CISO, die de coördinatie van de afhandeling op zich neemt.
- Hoog: het incident/probleem wordt door het IRT team afgehandeld. Het is hierbij altijd mogelijk om hoger op te schalen.

Bijlage 4 bij privacybeleid 2020 van de gemeenten Bunschoten, Leusden, Nijkerk en Putten

PROCEDURE DPIA

Deze procedure voorziet in het uitvoeren van Data Protection Impact Assessments (DPIA) ook wel Privacy Impact Assessments (PIA) genoemd.

Definities
Een DPIA is een risicoanalyse om de impact van een nieuwe gegevensverwerking, technologie, andere inrichting van de gegevensverwerkingen of andere invloed op de naleving of balans tussen rechten en vrijheden van betrokkenen te bepalen. Een DPIA biedt een instrument om te bepalen of de verwerking is toegestaan, of de impact van de verandering opweegt tegen negatieve gevolgen en of ingestelde waarborgen afdoende (kunnen) zijn om risico's en negatieve gevolgen te verminderen. Een goed uitgevoerde DPIA geeft inzicht in de risico's die de verwerking oplevert voor de betrokkenen, en in de maatregelen die de verantwoordelijke moet nemen om de risico's af te dekken.

Taken, verantwoordelijkheden en bevoegdheden
In de AVG wordt een DPIA verplicht gesteld in art. 35 AVG. Deze stelt: 'Wanneer een soort verwerking waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen voert verwerkingsverantwoordelijke vóór de verwerking een beoordeling uit van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens.' De verplichting geldt in het bijzonder wanneer nieuwe technologieën worden gebruikt of de aard, omvang, context en doeleinden een verhoogd risico opleveren, maar kan breder ingezet worden.

De AVG noemt enkele gevallen waarbij een DPIA uitgevoerd móet worden. Een daarvan betreft de grootschalige verwerking van bijzondere persoonsgegevens (art. 35 lid 3 sub b AVG).

Uitvoering procedure DPIA
Het proces uitvoeren DPIA start zodra een nieuwe verwerking van persoonsgegevens wordt ingericht, bestaande verwerkingen worden aangepast nieuwe technologieën worden gebruikt of nieuwe systemen worden aangeschaft. In deze gevallen worden in ieder geval volgende processtappen op hoofdlijnen doorlopen:

1. Signaal nieuwe gegevensverwerking
2. Advies FG aan proceseigenaar
3. Opdracht DPIA aan privacy beheerder
4. Uitvoeren DPIA QuickScan
5. Bepalen haalbaarheid compliance check dan wel uitvoering DPIA (IBD)
5. Uitvoering DPIA/Compliance check met behulp van DPIA-team

OPIA-team
Bepaal wie de DPIA gaat uitvoeren. Stel, afhankelijk van de grootte, een DPIA-team vast. Houd rekening met verschillende belangen zodat voldoende kennis en expertise aanwezig is, en de verschillende stakeholders en hun belangen vertegenwoordigd zijn. In een team zit bijvoorbeeld de manager afdeling, ICT-medewerker en uitvoerend medewerker. Voeg eventueel een onafhankelijke adviseur toe, zoals de FG.

Het DPIA-team bestaat uit volgende vaste leden:

Privacy beheerder
CISO
Proceseigenaar Projectleider
Uitvoerend medewerker

7. Beoordelen impact en bepalen maatregelen
Op basis van de ingevulde DPIA-vragenlijst en de risico's die daarbij naar voren zijn gekomen zal het DPIA-team de impact van de risico's bepalen en hierbij maatregelen benoemen die risico's wegnemen, wanneer de verwachte impact en risico's voor een betrokkene of organisatie te hoog zijn.

Bepaal de impact van een nieuwe verwerking na het treffen van de mitigerende maatregelen. Wanneer blijkt dat de verwerking een hoog risico oplevert, zelfs na het treffen van mitigerende maatregelen, zal de toezichthouder geraadpleegd moeten worden voordat gestart wordt met de verwerking (art. 36 lid 1 AVG, voorafgaande raadpleging).

8. Opstellen DPIA-verslag

Het verslag bevat de risico-inventarisatie, afwegingen, voorstellen voor maatregelen en conclusies. De DPIA bevat tenminste de volgende elementen (art. 35 lid 7 AVG):

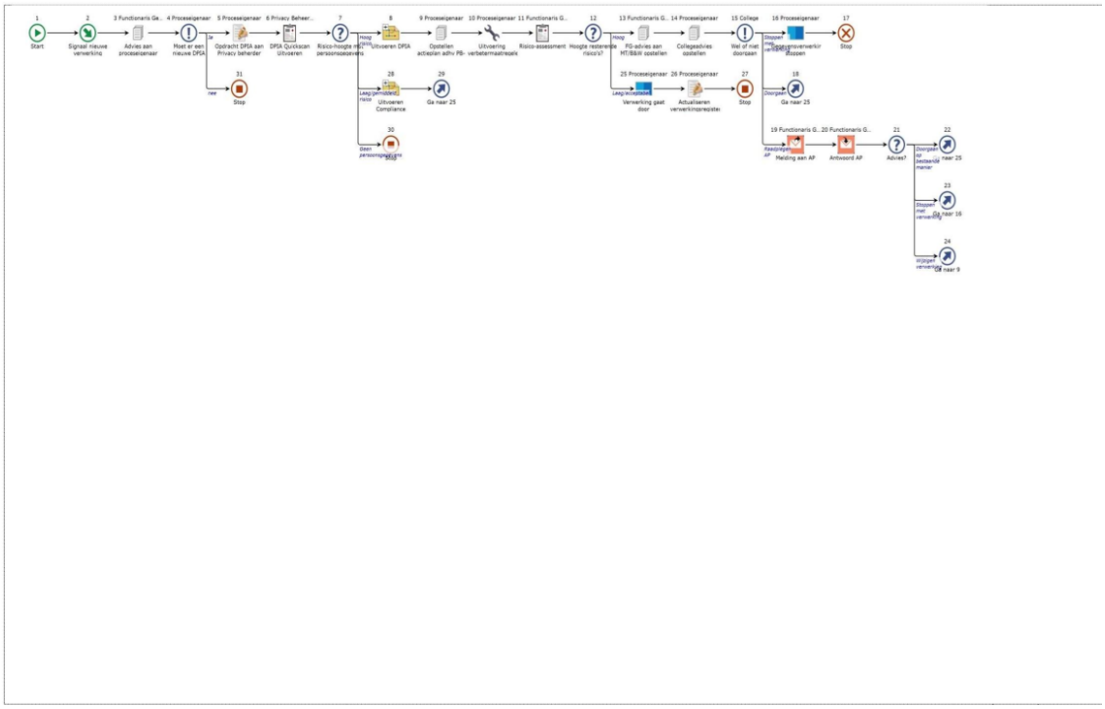
een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden, waaronder - in voorkomend geval - de gerechtvaardigde belangen die door de verwerkingsverantwoordelijke worden behartigd
een beoordeling van de noodzaak en de evenredigheid van de verwerkingen met betrekking tot de doeleinden
een beoordeling van de in art. 35 lid 1 bedoelde risico's voor de rechten en vrijheden van betrokkenen de beoogde maatregelen om de risico's aan te pakken, waaronder waarborgen, veiligheidsmaatregelen en mechanismen om de bescherming van persoonsgegevens te garanderen en om aan te tonen dat aan deze verordening is voldaan, met inachtneming van de rechten en gerechtvaardigde belangen van de betrokkenen en andere personen in kwestie

9. Check uitvoering verbetermaatregelen
Maatregelen die worden genomen op basis van de uitkomsten van de DPIA, zullen opgenomen moeten worden in een overzicht om de status en/of voortgang bij te kunnen houden. De FG van de gemeente dient een controle op de naleving van deze maatregelen uitvoeren.

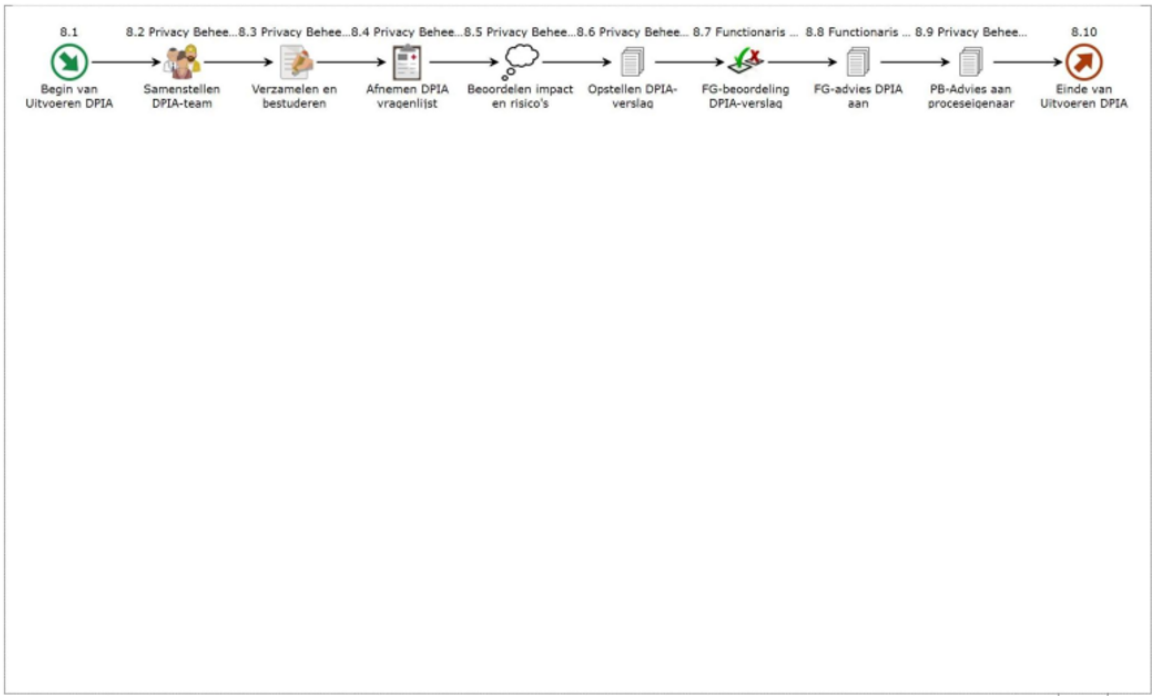
10. FG-beoordeling inclusief eventueel advies aan MT/B&W bij hoog resterend risico

11. Actualiseren verwerkingsregister

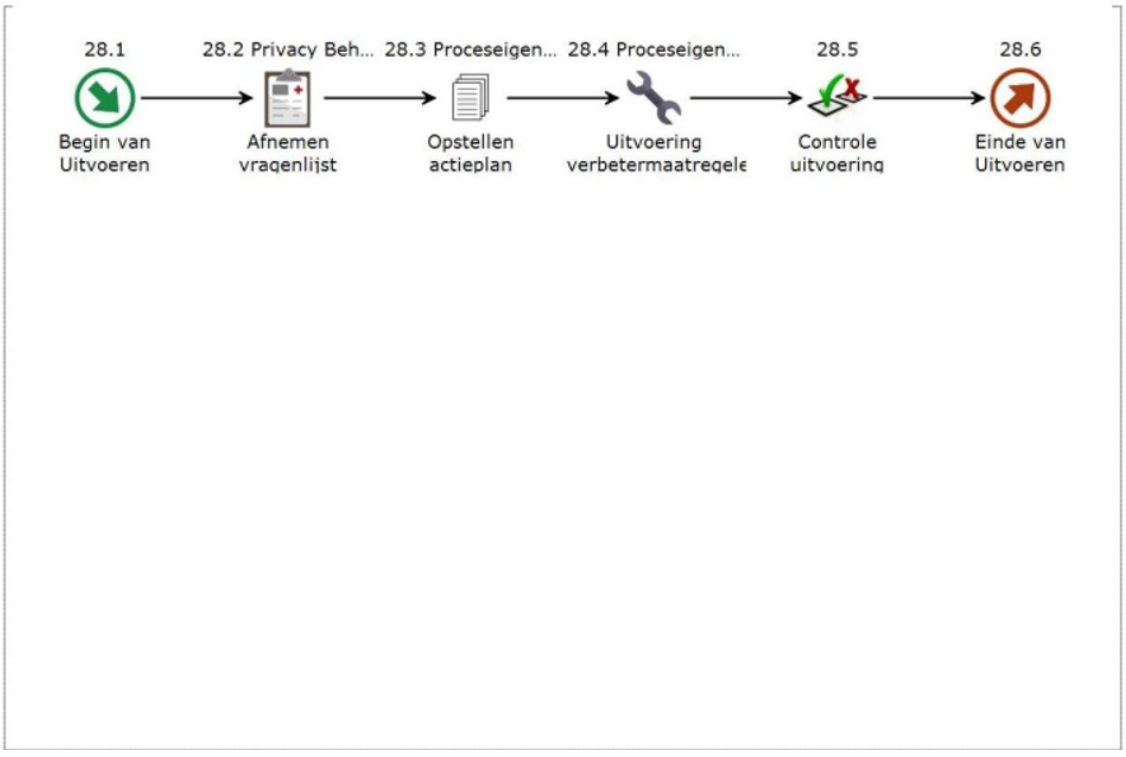
Zie bijgevoegd processchema voor een volledige procesbeschrijving.



Privacy Impact Assessment DPIA



Uitvoeren DPIA



Uitvoeren Compliance

Bijlage 5 bij privacybeleid 2020 van de gemeenten Bunschoten, Leusden, Nijkerk en Putten

Procedure Rechten Van Betrokkenen BLNP gemeenten

Afhandeling verzoeken op grond van AVG

Op 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. In de kern wil de AVG-betrokkenen in staat te stellen 'in control' te zijn over hun eigen persoonsgegevens. Zij krijgen meer en uitgebreidere rechten met betrekking tot hun persoonsgegevens en de verwerking daarvan. Nieuw zijn het recht op dataportabiliteit en het recht op vergetelheid. De overige rechten be stonden al onder de Wet bescherming persoonsgegevens. Betrokkenen hebben onder de AVG de volgende rechten:

1. Recht van inzage (artikel 15 AVG);
2. Recht op rectificatie (artikel 16 AVG);
3. Recht op vergetelheid (gegevenswissing) (artikel 17 AVG);
4. Recht op beperking van de verwerking (artikel 18 AVG);
5. Recht op dataportabiliteit (overdraagbaarheid gegevens) (artikel 20 AVG);
6. Recht van bezwaar tegen verwerking (artikel 21 AVG);
7. Recht niet te worden onderworpen aan geautomatiseerde individuele besluitvorming/profileren (artikel 22 AVG).

Betrokkenen hebben het recht om na te gaan wat er met hun persoonsgegevens gebeurt (punt 1) en hier als dit nodig is invloed op uit te oefenen (punt 2 t/m 7). Om betrokkenen nog meer in staat te stel len 'in control' te zijn, hebben verwerkingsverantwoordelijken daarnaast de verplichting om transparant te zijn door middel van een informatieplicht richting betrokkenen (artikel 13 en 14 van de AVG). De in formatieplicht hangt daarmee nauw samen met de rechten van betrokkenen: aan de ene kant is er de verplichting voor de gemeente om betrokkenen actief, tijdig en adequaat te informeren over verwerkin gen van persoonsgegevens; aan de andere kant kunnen betrokkenen hun rechten uitoefenen richting de gemeente.

Meer informatie over de verschillende rechten van betrokkenen staat op de website van de Autoriteit Persoonsgegevens: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie avg/rechten-van-betrokkenen

Met deze procesbeschrijving maken we inzichtelijk hoe om te gaan met verzoeken van rechten van betrokkenen.

Beslistermijn
De wettelijke beslistermijnen voor dit soort verzoeken zijn:
Artikel 12 lid 3 van de AVG
Besluit moet onverwijld maar in ieder geval binnen 1 maand verzonden worden, tenzij:
De complexiteit of het aantal verzoeken dusdanig groot is dat dit niet mogelijk is, dan mag de termijn verlengd worden met 2 maanden.
Dit artikel stelt verder dat meegewerkt moet worden aan elektronische verstrekking indien daarom gevraagd wordt.

Besluit
Alle rechten dienen wat procedure betreft op dezelfde manier afgehandeld te worden. De afhandeling eindigt in principe altijd met een besluit, tenzij het verzoek wordt ingetrokken (bijv. via minnelijke af handeling). Dataportabiliteit volgt dezelfde procedure maar is inhoudelijk erg verschillend. Bij alle an dere rechten vraagt een betrokkene aan een organisatie:
1. Welke gegevens heeft/verwerkt u van mij? en/of:
2. Ik wil dat u mijn gegevens corrigeert/ verwijdert/ niet langer verwerkt etc.

Een voorbeeld/ sjabloon van een dergelijk besluit is als bijlage opgenomen.

Opschorten/ verdagen
Als het niet mogelijk is om binnen 1 maand aan het verzoek te voldoen moet vóór afloop van de be slistermijn een verdagingsbrief gestuurd worden. De verdagingsbrief is weliswaar niet vatbaar voor be zwaar en beroep maar moet wél een motivering bevatten. Het is niet de bedoeling van de AVG dat alle verzoeken verdaagd worden. Neem dus altijd een motivering op die betrekking heeft op de om vang van het verzoek of de hoeveelheid ingekomen AVG-verzoeken. Dat zijn namelijk de 2 geldige re denen voor verdaging zoals genoemd in artikel 12 lid 3 AVG.

Bezwaar en beroep

Besluiten op AVG-verzoeken staan open voor bezwaar en beroep. Er moet dus een bezwarenclausule onder het besluit zijn opgenomen en er moet rekening gehouden worden met de afhandeling van inko mende bezwaren en/of beroepen.

Recht op dataportabiliteit
Het recht van dataportabiliteit geldt alleen voor niet-wettelijke taken van gemeenten en waarbij de vol gende voorwaarden van toepassing zijn:

- Het recht op overdraagbaarheid heeft betrekking op de gegevens die de betrokkene beschik baar heeft gesteld.
- Gemeenten wordt geadviseerd om zoveel mogelijk met uitwisselbare formats te werken om aan dergelijke verzoeken te voldoen. De ontvangende partij moet immers direct met de gegevens aan de slag kunnen.
- Controleer voor verzending àf en waarvoor de betrokkene toestemming heeft gegeven.
- De ontvangende gemeente dient alleen gegevens te accepteren die noodzakelijk en relevant zijn.

Wat betreft de formele afhandeling kan aangesloten worden bij de afhandeling zoals in het schema hierna weergegeven. Ook op dit soort verzoeken moet een besluit genomen worden.

Schema afhandeling verzoeken AVG

Afdeling	**Activiteit**
Postregistratie	- Binnenkomst verzoek (per postof Digid) - Registratie in zaaksysteem - Ter afhandeling naar betreffende vakafdeling/team - Ter registratie / kennisname in kopie naar privacy beheerder
Vakafdeling/team	- Ontvangst verzoek - Checken formele vereisten, eventueel termijn opschorten en mogelijk-heid tot herstel bieden - **Bezien of informele afhandeling mogelijk is** - Indien nodig ontvangst bevestigen en verdagen - Betreffende gegevens verzamelen en besluitvoorbereiden, indien no-dig jurist en/of Privacy beheerder betrekken - Besluit in mandaatondertekenen en verzenden
Vakafdeling	Afhandelen bezwaarschriften

Bijlage 1: Voorbeeld besluit

Datum: 14-2-2023

Geachte heer/mevrouw,

Aanvraag
Op [datum] hebben wij uw verzoek ontvangen om [inzage/ correctie/ vergetelheid etc.] op grond van artikel ... van de Algemene verordening gegevensbescherming (AVG).

U vraagt in uw verzoek het volgende:
' Indien mogelijk plak ik hier het liefst een passage uit het verzoek , dan kan er ook nooit tegengewor pen worden dat het verzoek verkeerd geïnterpreteerd is. Lukt dat niet of is dat in een specifiek geval niet handig , dan kun je het in eigen woorden samenvatten . '

Besluit
Wij hebben besloten uw verzoek [in te willigen/ te weigeren/ deels te weigeren]. Dit betekent dat wij *[concreet uitleggen wat er gedaan wordt, bijvoorbeeld: er wordt een overzicht verstrekt of de per soonsgegevens worden gecorrigeerd (of juist niet)].*

Optioneel : Voordat wij een kopie van uw persoonsgegevens/dossier kunnen meegeven , zijn wij ver plicht om *uw identiteit vast te stellen. Wij nodigen u daarom graag uit* om *een kopie van het complete dossier op te komen halen op het gemeentehuis in Nijkerk. Neem uw identificatiebewijs (Paspoort, Rij bewijs, ID kaart) mee zodat u zich kunt identificeren.*

[Indien van toepassing bij inzageverzoek]
In de bijlage treft u als antwoord op uw inzageverzoek de volgende informatie aan:

Overzicht van uw persoonsgegevens Doeleinden van de verwerking Categorieën van ontvangers Bewaartermijnen
Herkomst van uw persoonsgegevens
[Indien van toepassing bij inzageverzoek]

Motivering besluit
Persoonlijke werkaantekeningen vallen buiten het inzagerecht. Het moet dan wel gaan om per soonlijke aantekeningen. Wanneer aantekeningen bedoeld zijn om uit te werken in rapportages of als onderbouwing van het dossier in een bestand worden/zijn opgenomen, zijn het geen persoon lijke aantekeningen meer.
Inzage mag geweigerd worden als dat noodzakelijk is voor (art 23 AVG):

- de nationale veiligheid, landsverdediging en de openbareveiligheid;
- het voorkomen, opsporen en vervolgen van strafbare feiten;
- zwaarwegende economische en financiële belangen van Europese Unie, de staat en andere openbare lichamen;
- het toezicht op de naleving van wettelijke voorschriften die zijn gesteld om de onder 2 en 3 genoemde belangen te beschermen;
- bescherming van de onafhankelijkheid van de rechter en gerechtelijke procedures;
- de voorkoming, onderzoek, opsporing en de vervolging van schendingen van de beroepsco des voor gereglementeerde beroepen;
- een taak op het gebied van toezicht, inspectie of regelgeving die verband houdt, al is het inci denteel, met de uitoefening van het openbaar gezag in de gevallen, bedoeld in de bovenge noemde onderdelen;
- bescherming van uw rechten en vrijheden of die van anderen. Hier kan ook een onevenredige (administratieve) belasting van de organisatie onder vallen;
- de inning van civielrechtelijke vorderingen.

Bezwaar

Tegen dit besluit kan een belanghebbende bezwaar maken bij burgemeester en wethouders van Nijkerk. Het bezwaarschrift moet binnen zes weken na de verzenddatum van deze brief worden ingediend. Met een elektronische handtekening (DigiD) kan online bezwaar worden gemaakt via de web site www.nijkerk.eu/bezwaarmaken.

Met vriendelijke groet,

Namens burgemeester en wethouders van Nijkerk,

handtekening van de (onder)gemandateerde naam functionaris,

functiebenaming

Bijlage.
Bijlage bij besluit.

Overzicht
Hieronder treft u een overzicht aan van uw persoonsgegevens die wij hebben verwerkt in ons *[con tentbeheersysteem (Verseon/Djuma etc)]* en in ons papieren archief:

geslachtsomschrijving: heer/ mevrouw; uw voorletter;
uw roepnaam'; uw achternaam; uw adres;
uw e-mailadres; uw handtekening; Etc.

Wij hebben daarbij in acht genomen dat ook gegevens die, gezien de context waarin zij zijn geplaatst, direct dan wel indirect herleidbaar zijn tot de betreffende persoon, als persoonsgegevens dienen te worden aangemerkt. Wij concluderen dat wij naast het bovengenoemde, geen gegevens hebben verwerkt die wij dienen aan te merken als uw persoonsgegevens. Bovengenoemde persoonsgegevens zijn opgenomen in de volgende documenten, welke thans bij ons college berusten (origineel exemplaar of afschrift) en derhalve zijn verwerkt in ons geautomatiseerd systeem:

Een overzicht van de gevoerdecorrespondentie:
1. brief 1;
2. brief 2;

3. et cetera.

Doel(einden) van de verwerking en betrokken (categorieën van) persoonsgegevens
Uw naam, adresgegevens en e-mailadres zijn/worden verwerkt in ons geautomatiseerd systeem ten behoeve van de (elektronische) registratie en afhandeling van de door u ingediende documenten.

De door u aan ons toegezonden berichten/ documenten zijn na ontvangst ter registratie in het papieren archief opgenomen en gescand in ons geautomatiseerd systeem, waardoor naast uw geslacht, naam, adresgegevens en uw e-mailadres, tevens de in die documenten vermelde handtekening zijn verwerkt in ons geautomatiseerd systeem.

(Categorieën van) ontvangers
Uw persoonsgegevens hebben wij doen toekomen aan:
1. Uzelf, ter beantwoording van uw brieven, verzoeken, aanvragen en ingebrekestellingen;
2. Personen werkzaam voor gemeente Nijkerk belast met de afhandeling van de door u ingediende documenten;
3. *Externe partijen?*

De personen die werkzaam zijn binnen het gemeentehuis van de gemeente Nijkerk en geautoriseerd toegang hebben tot ons geautomatiseerd systeem, kunnen de genoemde persoonsgegevens raadplegen.

Bewaartermijn
De gemeente Nijkerk bewaart de uw persoonsgegevens niet langer dan strikt noodzakelijk is om de doelen te realiseren waarvoor uw gegevens worden verzameld. In sommige gevallen worden uw persoonsgegevens langer bewaard op grond van de Archiefwet.

Herkomst
[Alleen vullen als de persoonsgegevens niet van de betrokkene zelf komen].

Privacy rechten
Op grond van de AVG heeft u het recht om ons te verzoeken uw persoonsgegevens te corrigeren, verwijderen, de verwerkingen te beperken en het recht om bezwaar te maken tegen de verwerking. In dien u daarvan gebruik wenst te maken kunt u schriftelijk of per mail een verzoek indienen bij het col lege van burgemeester en wethouders. Wij zullen uw verzoek dan beoordelen.
Tevens hebt u het recht om een klacht in te dienen over de verwerking van uw persoonsgegevens bij de Autoriteit Persoonsgegevens.

Vragen
Voor vragen kunt u contact opnemen met [naam/team], bereikbaar op het in de aanhef van deze brief vermelde telefoonnummer of per e-mail [e-mail]