Gemeente Leusden

Jaarrapportage gegevensbescherming 2019

Gemeente Leusden

Jaarrapportage gegevensbescherming 2019

Deze jaarrapportage is bestemd voor zowel de gemeenteraad als het college van burgemeester en wethouders van de gemeente Leusden.

Deze rapportage betreft een interne toetsing aan de AVG van de verwerking van persoonsgegevens door (voornamelijk) het college van burgemeester en wethouders.

Mirjam Udo
Functionaris Gegevensbescherming
Juli 2020

Gebruikte formats:
Criteria Borging AVG en Jaarrapportage FG van VNG/IBD

Samenvatting

Op 25 mei 2018 werd de Algemene Verordening Gegevensbescherming (AVG) van kracht. De AVG verving de Wet bescherming persoonsgegevens (Wbp) en zorgt voor een verhoogde aandacht voor een rechtmatige verwerking van persoonsgegevens in alle sectoren. De overheid heeft hierin een belangrijke voorbeeldfunctie. Dit jaarverslag geeft de situatie weer met betrekking tot de gegevensverwerking in 2019.

Invloed ontwikkelingen in samenleving op privacy
Nu ons leven inmiddels beheerst wordt door de coronacrisis, zal dit ook de aard en wijze van de bescherming van persoonsgegevens beïnvloeden. Wat dit concreet zal betekenen voor het naleven van de AVG en andere privacyregelgeving is op voorhand lastig te duiden. De bescherming van persoonsgegevens zal in velerlei opzicht een blijvende alertheid en wendbaarheid vragen, waarop de gemeentelijke organisatie goed zal moeten worden toegerust.

Privacy binnen BLNP bedrijfsvoering samenwerking
In 2019 werkten ontwikkelingen in de samenleving, vooral waar die samen gaan met verder toenemende digitalisering, intensief in op vrijwel alle gemeentelijke organisatieprocessen. De urgentie om hier als gemeente in mee te bewegen en goede waarborgen te bieden voor de bescherming van persoonsgegevens wordt daardoor steeds groter. De gemeente Leusden heeft hierin nog stappen te zetten maar is ook op de goede weg, bijvoorbeeld door in te zetten op beveiliging van data, inclusief de persoonsgegevens en daarbij nauw samen te werken met de gemeenten Bunschoten, Leusden en Putten. Dit gebeurt vanuit het team Informatisering van het bedrijfsvoering samenwerkingsverband BLNP (I-kernteam). Privacybescherming maakt daarbij deel uit van de taken die zijn onder gebracht bij de gastheergemeente voor ICT, de gemeente Bunschoten.

Privacybescherming binnen lokale operationele processen
Privacybescherming is nauw gerelateerd aan Informatieveiligheid maar strekt zich uit over een breder terrein dan alleen Informatisering. Privacybescherming geschiedt vooral binnen de operationele bedrijfsprocessen, waarvoor de lokale leidinggevenden/proceseigenaren in eerste instantie verantwoordelijk zijn en uiteindelijk de bestuursorganen raad, college van burgemeester en wethouders en de burgemeester, die zich hierover ook dienen te verantwoorden. Meer inzicht in de gemeentelijke processen waarbinnen persoonsgegevens verwerkt worden en hoe daarbij eventueel wordt samengewerkt met andere partijen is noodzakelijk. Ook is noodzakelijk dat de gemeente lokaal verantwoordelijkheden belegt voor de uitvoering van de AVG en aanverwante wetgeving en kan aantonen hoe hieraan invulling gegeven wordt binnen de organisatie.

Samenvatting werkzaamheden bescherming persoonsgegevens in 2019
Adequaat omgaan met persoonsgegevens is kortom een blijvend proces dat de aandacht zal blijven vergen van zowel bestuur, management als medewerkers. Samenvattend is in 2019 voor de gemeente Leusden veel werk verzet op het gebied van bescherming van persoonsgegevens. Het ging daarbij onder andere om:

- Het na een risico inventarisatie door de privacybeheerders BLNP, in overleg met de Functionaris Gegevensbescherming (FG, de interne toezichthouder wat betreft de naleving van de AVG en contactpersoon voor de externe toezichthouder, de Autoriteit Persoonsgegevens) opstellen en deels uitvoeren van het Privacy Jaarplan 2019;

- Het opstellen van een concept voor een BLNP breed Privacy beleid met als bijlagen o.a. een Informatie veiligheids- en Privacy governance document (taken en rollen) en diverse procedures en formats, zoals een procedure voor de afhandeling van informatie veiligheids-incidenten/datalekken;

- Ondersteuning en advies aan bestuur, management en medewerkers door de lokale privacy beheerder, in overleg met betrokken teams of functionarissen, zoals de Chief Information Security Officer (de CISO BLNP en de lokale CISO, dit zijn de informatieveiligheidsadviseurs) en de FG;

- Overleg tussen de FG en de regiegroep (gemeentesecretarissen in BLNP-verband), met de gemeentesecretaris van Leusden afzonderlijk of met procesverantwoordelijken in Leusden over de BLNP-brede of lokale aandachtspunten en dilemma's rond privacy. Dit betrof onder meer de voortgang van het te voeren privacy beleid en daarbij te stellen prioriteiten, de afhandeling van (vermeende) datalekken en technische en organisatorische maatregelen in verband met de bescherming van persoonsgegevens binnen de gemeente;

- AVG-informatiebijeenkomsten:
  In 2018 richtten deze zich op vertegenwoordigers uit bestuur en management, controllers en diverse (groepen) medewerkers. In 2019 was er daarnaast vooral via de BLNP regiegroep (bestaande uit de vier gemeentesecretarissen) afstemming met de FG over de voortgang van de implementatie van de AVG binnen de organisaties. In dat kader vonden ook diverse bijeenkomsten en (werk)overleggen plaats, waaronder:
  - een informatie bijeenkomst (17-4-2019) voor de gemeentesecretarissen en beoogde (coördinerend) proceseigenaren privacy over de borging van de AVG binnen BLNP;
  - een workshop-middag over privacy (01-07-2019) in relatie tot risicoleiderschap voor de collegeleden, proceseigenaren en controllers binnen BLNP. Naast privacy- en risicomanagementexperts, gaven ook medewerkers Informatieveiligheid BLNP voorlichting over bedreigingen en maatregelen op het gebied informatieveiligheid/privacy;

- Informatie over privacy op de gemeentewebsite (bij privacyverklaring) en op de intranetten van de BLNP-gemeenten, waaronder een privacy nieuwsbrief en links naar protocollen en formats;

- Deelname aan diverse overleggen intern en binnen samenwerkingsverbanden waarin Leusden vertegenwoordigd is. Dit gebeurt door de lokale privacy beheerder en de FG met diverse teams/medewerkers en derden, zoals het BLNP team Informatisering BLNP, het BLNP CISO-team en het FG- en CISO-overleg tussen de gemeenten Amersfoort, Baarn, Bunschoten, Soest en Woudenberg;

- Uitvoeren van wettelijk verplichte gegevens bescherming effectbeoordelingen en andere privacy scans. Dit betrof o.a. leerlingen vervoer in de BLNP-gemeenten, het zaaksysteem van Putten, dat ook in Nijkerk wordt toegepast, het financieel systeem waarvoor de gemeente Leusden als gastheer financiën regie voert en de privacy quick scan door onderzoeksbureau BMC met betrekking tot het sociaal domein binnen de vier BLNP-gemeenten afzonderlijk;

- Investeren in opleidingen en cursussen voor o.a. de privacy beheerder, de FG en de griffie.

Gemeente Leusden

Inhoudsopgave

Bijlagen:
1: Stand van zaken AVG Leusden per onderwerp
2. Overzicht incidenten met persoonsgegevens in Leusden in 2019

Inleiding

Doordat het coronavirus het dagelijks leven nu volop is gaan beheersen, is het werk bij de gemeenten logischerwijs grotendeels in het teken van deze uitzonderlijke situatie komen te staan. Ook privacybescherming is hierdoor, nog meer dan voorheen, een publieke zaak geworden. Meebewegen met ontwikkelingen door zorgvuldig overheidshandelen is daardoor nog belangrijker geworden.

Dit Jaarverslag heeft echter betrekking op 2019, een periode waarin de naleving van de AVG, verder zijn beslag diende te krijgen om daarmee het grondrecht op bescherming van persoonsgegevens te kunnen waarborgen. De gemeente Leusden geeft in verband daarmee op haar website ook aan dat mensen van wie de gemeente persoonsgegevens verwerkt er ook op mogen vertrouwen dat dit zorgvuldig en vertrouwelijk verloopt, zie: https://www.leusden.nl/privacy.html

AVG: zorgvuldig omgaan met persoonsgegevens
Dit betekent dat de gemeente ook dient te investeren in het zorgvuldig omgaan met persoonsgegevens. Gemeenten verwerken bij de uitoefening van hun taken veel informatie. Niet alleen persoonlijke informatie van eigen inwoners, maar ook van medewerkers, externen en partijen waarmee wordt samengewerkt.
De AVG vormt, met de Uitvoeringswet AVG (UAVG) en sectorale privacywetgeving, het wettelijk kader voor het verwerken van persoonsgegevens. De AVG stelt dat de gemeente transparant dient te zijn over welke persoonsgegevens zij verwerkt en voor welk doel. Persoonsgegevens mogen alleen worden verwerkt wanneer dit in overeenstemming is met het doel waarvoor zij zijn verzameld en gegevens mogen niet langer bewaard worden dan strikt noodzakelijk. Bovendien moet de gemeente, ook in het kader van de BIO (Baseline Informatieveiligheid Overheden), passende technische en organisatorische beveiligingsmaatregelen treffen om onrechtmatige toegang tot deze persoonsgegevens tegen te gaan en daardoor een onrechtmatig gebruik van deze persoonsgegevens te voorkomen. Dit alles heeft gevolgen voor de inrichting van processen en systemen binnen de gemeente.

De gemeenteraad
De gemeenteraad is als zelfstandig verwerkingsverantwoordelijke verantwoordelijk voor de verwerking van persoonsgegevens door de raad en de griffie. Dit betekent dat de gemeenteraad moet kunnen aantonen dat de verwerkingen door/namens de raad voldoen aan de AVG. Daarnaast dient de raad onder andere een register van de verwerkingsactiviteiten bij te houden en technische en organisatorische maatregelen te nemen om persoonsgegevens te beschermen. Verder zullen, wanneer er door/namens de raad persoonsgegevens verstrekt worden aan andere partijen, hierover specifieke afspraken moeten worden gemaakt.

Dit FG jaarverslag is bedoeld voor zowel de raad als het college. Beide jaarverslagen voor 2019 zijn dus samen gevoegd. Dit is gedaan omdat veruit de meeste verwerkingsactiviteiten door of namens de gemeente geschieden onder de verantwoordelijkheid van het college, waardoor de focus in 2019 vooral gelegd is op deze verwerkingen. De verwerkingen van de gemeenteraad zijn tot dusver zo goed mogelijk via de griffie geborgd. De gemeenteraad kan in de toekomst, als zelfstandig

verwerkingsverantwoordelijke en als controlerend orgaan van het college van B&W, separaat een eigen FG jaarverslag ontvangen.
De verwerkingen van de raad en de griffie zijn via de griffie, tot dusver opgenomen in het gemeentelijke register van verwerkingsactiviteiten. Dit register kunt u terugvinden op de gemeentewebsite, zie:
https://www.leusden.nl/fileadmin/user_upload/Bestanden/Documenten/Over_deze_website/Def.register-Leusden_17072018_publicatieversie_v1.0.pdf.

De raad kan ook besluiten om een eigen register van verwerkingsactiviteiten bij te (laten) houden. In samenwerking met de Vereniging van Griffiers stelde de Informatie Beveiligings Dienst (IBD) een document op met concrete voorbeelden uit de praktijk van de gemeenteraad. Dit document kan dienen als afwegingskader bij de omgang met persoonsgegevens, zie:
https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2019/07/Casuistiek-gegevensbescherming-gemeenteraad.pdf

Voor de griffies heeft in 2019 in BLNP-verband een AVG training plaats gevonden, gevolgd door een vervolgbijeenkomst in verband met het kunnen borgen van privacybescherming en het bespreken van privacy issues. Voor de gemeenteraad van Leusden is een document beschikbaar waarin staat hoe vanuit de raad/griffie wordt omgegaan met persoonsgegevens. Dit wordt momenteel geactualiseerd.

Het college/de burgemeester
Het college van Burgemeester en Wethouders (hierna: het college) is verwerkingsverantwoordelijke voor het merendeel van de verwerkingen van persoonsgegevens binnen de gemeente en de burgemeester voor de verwerkingen die tot zijn taak behoren. Dit brengt veel verplichtingen met zich mee. In deze jaarrapportage staat beschreven welke acties en maatregelen de gemeente Leusden in 2019 -grotendeels in BLNP-verband- heeft genomen om de doelstellingen en beginselen uit de AVG te behalen en te borgen. Ook bevat dit document aandachtspunten en actiepunten voor het jaar 2020. Onder de verantwoordelijkheid van het college vindt een groot aantal verwerkingen van persoonsgegevens plaats. Het gaat hierbij om persoonsgegevens van eigen inwoners, inwoners van andere gemeenten, zakenrelaties, medewerkers en externen.

Extern en intern toezicht op privacyregels
De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de privacyregels in Nederland, zie: https://autoriteitpersoonsgegevens.nl/. Daarnaast dient de gemeente Leusden te beschikken over een interne toezichthouder: de Functionaris voor de Gegevensbescherming (FG). Op 1 mei 2018 is door middel van de benoeming van een FG in de gemeente Bunschoten, ten behoeve van de bedrijfsvoering samenwerking tussen de gemeenten Bunschoten, Leusden, Nijkerk en Putten (BLNP) voorzien in deze wettelijke verplichting. De formele aanstelling van de FG door de bestuursorganen[1] van gemeente Leusden dient nog wel plaats te vinden.
De FG ziet erop toe dat de AVG intern wordt nageleefd en het college moet ervoor zorgen dat de FG naar behoren en tijdig wordt betrokken bij alle gelegenheden die verband houden met de bescherming van persoonsgegevens. De FG moet daarom toegang worden gegeven tot de persoonsgegevens en de verwerking daarvan en over de nodige middelen kunnen beschikken om deze taak te kunnen uitvoeren, waaronder opleidingsfaciliteiten.

[1] Hiermee worden de drie bestuursorganen van de gemeente bedoeld: de burgemeester, het college van burgemeester en wethouders en de gemeenteraad.

Met ingang van dit verslag over 2019, zal voortaan jaarlijks een FG-jaarverslag worden uitgebracht aan de verwerkingsverantwoordelijken van de verrichte werkzaamheden, bevindingen en aanbevelingen.

Leeswijzer

Deze jaarrapportage bestaat uit twee onderdelen.
In het eerste deel wordt teruggekeken naar het jaar 2019. Wat heeft de gemeente bereikt op het gebied van gegevensbescherming? Welke maatregelen zijn er genomen om te voldoen aan de AVG?
In het tweede deel worden aanbevelingen gedaan om gegevensbescherming en privacy in het jaar 2020 naar een nog hoger niveau te tillen. Hierbij wordt waar nodig ook aandacht geschonken aan de technische en organisatorische middelen die nodig zijn om dit hogere niveau te bereiken.

De criteria die in beide delen worden genoemd zijn afkomstig uit het document ‘Het borgen van de Algemene Verordening Gegevensbescherming in de gemeentelijke organisatie’ van de Informatiebeveiligingsdienst. In dit document worden criteria en maatregelen omschreven die de AVG vertalen zijn naar een kwaliteitscyclus voor gegevensbescherming en privacy voor gemeentelijke processen. In en in bijlage 1 is een overzicht opgenomen waar in cirkeldiagramvorm wordt aangegeven in hoeverre de gemeente de AVG-criteria reeds heeft geïmplementeerd en in bijlage 2 is een overzicht opgenomen van de incidenten met persoonsgegevens in Leusden in 2019.

Deel 1. Terugblik op 2019

In dit deel van de rapportage zal worden teruggeblikt op wat de gemeente in 2019 heeft bereikt en welke werkzaamheden zijn verricht.

1. Privacybeleid

Het concept privacybeleid voor de gemeente Leusden is 2019 in BLNP-verband ontwikkeld en is in mei 2020 vast gesteld door het college. Het beleid bestaat uit een beschrijving van de manier waarop de BLNP-gemeenten toepassing zullen geven aan de AVG en aanverwante privacywetgeving. Hiervoor relevante bijlagen zijn vooral:

Bijlage 1.	Governance BLNP (inrichting privacy-organisatie en samenhang tussen sturing, uitvoering en verantwoording)
Bijlage 2.	Uitwerking begrippen AVG (kernbegrippen en verhouding tot andere wetten)
Bijlage 3.	Procedure Incidentmanagement en Respons (incl. procedure datalekken)
Bijlage 4.	Procedure DPIA (Data Protection Impact Assessment of gegevens beschermings effectbeoordeling)
Bijlage 5.	Procedure Rechten van Betrokkenen (procedure om personen van wie persoonsgegevens worden verwerkt hun rechten te kunnen laten uitoefenen)

In de overige bijlagen zijn verdere procedures voor de (praktische) uitvoering van de AVG opgenomen.

2. Processen

De verwerkingen van persoonsgegevens van de gemeente Leusden dienen te voldoen aan de AVG. Dit houdt in dat de werkprocessen die persoonsgegevens bevatten, getoetst en ingericht moeten worden volgens de volgende beginselen: behoorlijkheid, transparantie, doelbinding (of de verwerking in overeenstemming is met het doel waarvoor de persoonsgegevens zijn gegeven), dataminimalisatie (er mogen niet meer gegevens worden verwerkt dan noodzakelijk), opslagbeperking, juistheid, integriteit (de gegevens moeten juist, volledig en actueel zijn) en vertrouwelijkheid (de gegevens mogen alleen in handen komen van bevoegde personen).

Register van verwerkingsactiviteiten
In het register van verwerkingsactiviteiten staan de verwerkingen waarvoor de gemeente zelf verantwoordelijk is of medeverantwoordelijk voor is, zoals opgenomen in diverse werkprocessen. Het register bevat ten minste de volgende gegevens:
- de naam en de contactgegevens van de verwerkingsverantwoordelijke, eventuele gezamenlijke verwerkingsverantwoordelijken en van de FG;
- de verwerkingsdoeleinden;

- de categorieën van betrokkenen en categorieën persoonsgegevens;
- de categorieën van ontvangers;
- of de gegevens worden doorgegeven aan een derde land of een internationale organisatie;
- de bewaartermijnen;
- de beveiligingsmaatregelen.

In 2019 is door een ingehuurde medewerker een actualisatie van het register gestart, die doorloopt tot in 2020.

3. Organisatorische inbedding

Voor een goede uitvoering van privacy taken is het van belang dat een ieder binnen de organisatie op de hoogte is van de beginselen van de AVG en het belang van privacybescherming binnen zijn of haar taak. Een goede organisatorische inbedding betekent het toewijzen van taken, verantwoordelijkheden en bevoegdheden en ook privacy bewustzijn bevorderen. Dit is een management-verantwoordelijkheid. De verantwoordelijke managers/proceseigenaren kunnen in het kader van de borging van de AVG in de organisatie gebruik maken van de adviezen van de FG en voor de uitvoeringspraktijk van de adviezen van en ondersteuning door de privacy beheerder(s).

Er is bereidheid tot samenwerking tussen de (BLNP) functionarissen voor informatiemanagement, informatieveiligheid, privacybeheerders en FG. Deze samenwerking moet om de AVG goed te kunnen borgen, wel beter worden georganiseerd, minder vrijblijvend. Er moet daarnaast wordt samengewerkt met veel anderen, binnen en buiten de organisaties. Een structurele en logische taakverdeling is een vereiste om de beveiliging van data, inclusief de persoonsgegevens, op een hoger plan te brengen. Door gerichter samen te werken kunnen ook kosten worden bespaard, b.v. door een gezamenlijke Informatieveiligheids- en privacy-monitoringcyclus (PDCA) te ontwikkelen om risico's te kunnen wegen en daarop te kunnen sturen, door zoveel mogelijk gezamenlijk procedures te ontwikkelen en door benodigde systemen gezamenlijk aan te schaffen.

Privacybescherming maakt deel uit van de taken die zijn onder gebracht bij de gastheergemeente voor Informatisering/ICT, de gemeente Bunschoten en vergt voldoende capaciteit en middelen. De capaciteit voor de FG-taak moet onder normale werkomstandigheden toereikend zijn. In 2019 was daarvan nog geen sprake door een veelheid aan organisatorische kwesties binnen de BLNP-gemeenten en het BLNP samenwerkingsverband. De AVG is echter op 25 mei 2016 in werking getreden, waarbij organisaties 2 jaar de tijd kregen om zich organisatorisch voor te bereiden om hieraan te kunnen voldoen, zie: https://europadecentraal.nl/algemene-verordening-gegevensbescherming-treedt-in-werking-op-25-mei-2016/. Nog steeds legt dit onderwerp het vaak af tegen andere prioriteiten. Hoe begrijpelijk soms ook, is dit in deze tijd wel risicovol voor zowel betrokkenen (burgers, medewerkers, derden met wie wordt samengewerkt) als voor de organisaties zelf.

ISMS

De aanschaf van een Information Security Management System (ISMS) maakt het toepassen van risicomanagement mogelijk door middel van het monitoren en kunnen inspelen op ontwikkelingen binnen het aandachtsgebied informatieveiligheid en privacybescherming. Hierin is nog niet voorzien. In het kader van de Informatieveiligheidsregelgeving, de Baseline Informatieveiligheid Overheden

(BIO) is het hanteren van een ISMS verplicht voor overheden. De aanschaf van een ISMS is heel goed mogelijk in BLNP-verband. Dit bespaart kosten en tijd. Het ISMS geeft de betrokkenen binnen de informatieveiligheid en privacy governance inzicht in de actuele stand van zaken en biedt ook mogelijkheden om als gemeenten van elkaar te leren.

DPIA's

De gemeente kan, in bepaalde gevallen, verplicht zijn om een gegevens beschermings-effectbeoordeling (DPIA[2]) uit te voeren. Dit is een instrument om vooraf de privacy risico's in kaart te kunnen brengen bij risicovolle verwerkingen. Vervolgens kunnen maatregelen genomen worden om de risico's te verkleinen. Het gaat om privacy risico's binnen processen waarvoor de organisatie verantwoordelijk is, bijvoorbeeld door het aangaan of wijzigen van een samenwerkingsverband of het toepassen van een nieuw systeem met impact op de verwerking van persoonsgegevens. In 2019 is BLNP-verband een eerste DPIA uitgevoerd op de werkprocessen rondom het leerlingen vervoer. In verband met de aanschaf van een nieuw systeem voor de werkprocessen rondom de uitvoering van de Leerplicht wet en het leerlingen vervoer, dient in 2020 een aanvullende privacy scan of nieuwe DPIA te worden uitgevoerd.

Via de regiegroep van gemeentesecretarissen BLNP is in 2019 het FG advies gegeven om in de vier organisaties ieder geval een DPIA te laten voeren voor:
- het zaaksysteem (systeem voor registratie van de werkvoorraad)
- het HRM-systeem Youforce en werkprocessen binnen HRM
- het cameratoezicht in de openbare ruimte, de camerabewaking van gemeente-eigendommen en het eventueel toepassen van monitoring van medewerkers door middel van camera's.

DPIA's in BLNP verband

Voor Putten is een DPIA uitgevoerd met betrekking tot het zaaksysteem Djuma, dat ook in gebruik is bij de gemeente Nijkerk. Inmiddels zijn de meeste geadviseerde verbeterpunten ten aanzien van dit systeem in Putten doorgevoerd en deels ook in Nijkerk. Leusden en Bunschoten hanteren een ander zaaksysteem. Voor dat van Leusden is inmiddels een aantal verbeteringen doorgevoerd, waardoor de maatregelen die volgen uit een DPIA mogelijk beperkt zullen zijn.
In Leusden is in 2019 uitvoering gegeven aan een DPIA voor het financiële systeem Key2financiën, waarvoor Leusden de gastheergemeente is. Ook hierbij zijn de meeste adviezen ter verbetering inmiddels opgevolgd, voor zover binnen het bereik van het team Financiën.
Aan de DPIA voor HRM is in Nijkerk (gastheer HRM in BLNP verband), in 2019 nog geen prioriteit gegeven. Dit was in 2019 in de vier gemeenten evenmin het geval met betrekking tot de DPIA's rond cameratoezicht, -bewaking en –monitoring.

Rol FG bij DPIA's

Op grond van artikel 38 lid 1 AVG dient te FG door de verwerkingsverantwoordelijke (college) naar behoren en tijdig betrokken te worden bij *alle* aangelegenheden die verband houden met de bescherming van persoonsgegevens en artikel 35 lid 2 AVG verplicht het college om het advies van de FG in te winnen bij het uitvoeren van de DPIA. Ten aanzien van het uitvoeren van DPIA's raadt de Europese groep van privacytoezichthouders de verantwoordelijke (college) aan onder andere over de volgende zaken het advies van de FG in te winnen:

[2] De gegevensbeschermingseffectbeoordeling wordt ook wel afgekort tot DPIA naar de Engelse term Data Protection Impact Assessment.

• of er al of niet een DPIA uitgevoerd moet worden;
• welke methodiek voor de DPIA gebruikt moet worden;
• of de DPIA intern uitgevoerd of uitbesteed moet worden;
• welke waarborgen (zoals technische en organisatorische maatregelen) ingebouwd moeten worden om eventuele risico's voor de rechten en belangen van de betrokkenen te beperken;
• of de DPIA correct uitgevoerd is en de conclusies daaruit (de vraag of de verwerking door moet gaan en welke waarborgen er ingebouwd moeten worden) aan de AVG voldoen.

Indien de verantwoordelijke het niet met het advies van de FG eens is, dient in de documentatie van de DPIA specifiek schriftelijk aangegeven te worden waarom het advies niet overgenomen is.

Privacy Quick Scan Sociaal Domein
Verder is met betrekking tot het sociaal domein in BLNP verband het FG advies gegeven om in 2019 binnen de vier gemeenten afzonderlijk een privacy quick scan te laten plaatsvinden. Dit advies is in dat jaar ook opgevolgd door middel van een opdracht aan adviesbureau BMC. Voor Leusden volgden hieruit globaal de volgende aandachtspunten:

1. Leg de spelregels rond integraal werken en samenwerking met andere taakvelden (zoals openbare orde en veiligheid) en partijen (zoals Lariks en Stadsring 51), helder vast. Let op het waarborgen van informatieveiligheid bij het in mandaat namens de gemeente verwerken van persoonsgegevens. Veranker dit in beleid en afsprakenkaders/protocollen/formats;
2. Stap af van 'toestemming' van de betrokkene als basis om met andere partijen te gaan overleggen. De reden hiervan is dat toestemming als verwerkingsgrondslag alleen kan als deze toestemming vrijelijk kan worden gegeven. Dat is binnen het sociaal domein maar heel beperkt mogelijk. Deel het de betrokkene mede (transparantiebeginsel) en stel een procedure op voor als betrokkene weigert;
3. Let op het rechtmatig verwerken van het BSN nummer;
4. Stel autorisatiebeleid vast en zie toe op het toepassen van de juiste autorisaties vooral bij uit- en doorstroom van medewerkers bij alle applicaties en check deze geregeld;
5. Stel logging beleid vast en maak gebruik van de logging door hier regelmatig controles op uit te oefenen. Vooral waar autorisaties breed zijn ingeregeld (gebiedsteams) en dus meer controle nodig is Let op instemmingsbevoegdheid van de Ondernemingsraad (WOR artikel 27 lid 1 onder k); Inmiddels wordt hiervoor een concept uitgewerkt binnen Informatieveiligheid dat wordt besproken met de FG en andere betrokkenen;
6. Voer waar nodig DPIA's uit, zoals in geval van werken in samenwerkingsverbanden met derden.

Privacy risico's overige gemeentelijke domeinen
Processen binnen de andere gemeentelijke domeinen: bestuur, ruimte, publieksdiensten, openbare orde en veiligheid en ondersteuning zijn weliswaar geïnventariseerd in het kader van het opstellen van het register van verwerkingsactiviteiten maar dit betrof geen privacy scan zoals binnen het sociaal domein is uitgevoerd.
Hierdoor ontbreekt nog grotendeels een dieper inzicht in privacy aspecten/-risico's in de werkprocessen binnen deze domeinen. Onduidelijk is hierdoor in hoeverre nog in noodzakelijke aanpassing of uitwerking van afspraken, protocollen en overige documenten moet worden voorzien.

Invulling privacy governance

Al onder het regime van de voorganger van de AVG, de Wet bescherming persoons-gegevens moest privacybescherming zijn beslag hebben gekregen binnen de organisatie. Hieraan was slechts ten dele uitvoering gegeven. Gezien de vele samenwerkingsverbanden en het onregelmatige niveau van privacy volwassenheid binnen de organisatie(s) is het implementeren van de AVG in Leusden een omvangrijke taak.

In 2019 was bovendien de privacy governance binnen de BLNP gemeenten, die in 2017 is vastgesteld in het kader van het Informatieveiligheidsbeleid, nog maar ten dele ingevuld.

In 2019 was in Leusden de privacy governance als volgt ingevuld:

FG:	32 uur voor de vier gemeenten Taken globaal: strategisch advies (vooral aan gemeentesecretaris/colleges), intern toezicht, contactpersoon betrokkenen en Autoriteit Persoonsgegevens, zie voor een uitgebreidere taakomschrijving van de gemeentelijke FG: https://www.informatiebeveiligingsdienst.nl/nieuws/nieuwe-handreiking-privacy-positionering-rol-en-taken-fg/
Privacybeheerder:	18 uur vaste formatie, inclusief de taken in BLNP verband. Taken globaal: operationeel advies en ondersteuning (bij gebrek aan proceseigenaren privacy gebeurde dat vooral aan diverse medewerkers, de gemeentesecretaris en de portefeuillehouders binnen het college), bijhouden van het register van verwerkingen, informatie en advies bij datalekken, betrokken bij de ontwikkeling van privacy borging in BLNP-verband, zoals het opstellen van het privacy jaarplan en het uitvoeren van DPIA's.
Coördinatie privacy-Beheer in BLNP verband:	4 uur vaste formatie, de privacybeheerder Leusden vervult sinds 2020 een coördinerende rol binnen het team van privacybeheerders BLNP, bovenop de 18 uur voor Leusden
Coördinerend proces-Eigenaar informatie-Veiligheid/Privacy:	in 2019 en tot dusver in 2020 nog niet ingevuld (in 2020 is deze taak wel deels waargenomen door de organisatie directeur a.i.) Taken globaal: zorgen voor borging privacy beleid binnen de teams (personele capaciteit, bedrijfsprocessen en –systemen) en afstemming met collega coördinerend proceseigenaren BLNP
Proceseigenaren Informatieveiligheid/ Privacy voor Bestuur; Ruimte; Sociaal Domein Publieksdiensten; Openbare Orde en Veiligheid en voor	

Ondersteuning:	In 2019 nog niet ingevuld Taken globaal: idem als coördinerend proceseigenaar maar dan gericht op het betreffende vakgebied
Aandachtsfunctionaris privacy in teams:	In 2019 nog niet ingevuld Taken globaal: beheer, de coördinatie en advies ten aanzien van privacybescherming van specifieke gegevensverzamelingen

Gezamenlijke aanpak privacy taken in BLNP-verband versus lokale aanpak
De gezamenlijke aanpak in BLNP verband heeft in 2019 geleid tot de in de samenvatting op blz. 3-5 opgesomde werkzaamheden. Het ontwikkelen en borgen van (vak gerelateerd) privacy beleid binnen de teams van de gemeente Leusden is door de privacy beheerder, vooral op ad hoc basis, zo goed als mogelijk was, opgepakt binnen de domeinen bestuur, sociaal domein, ruimte, publieksdiensten, openbare orde en veiligheid en ondersteuning. Ook is daarbij aandacht besteed aan privacy bewustwording. De aandacht ging vooral uit naar het sociaal domein vanwege de gevoeligheid van de daarbinnen te verwerken persoonsgegevens en acties die volgden uit incidenten met persoonsgegevens, onder meer in verband met samenwerking met andere organisaties. De medewerkers binnen de organisatie wisten de privacy beheerder tot dusver goed te vinden voor advies en ondersteuning.

Juridische Zaken
Het team Juridische Zaken (JZ) adviseerde in 2019 nauwelijks ten aanzien van privacy issues die in Leusden spelen. JZ is niet vertegenwoordigd binnen het privacy team van privacybeheerders en FG. Het team JZ heeft vanwege de brede adviestaak, beperkt ruimte voor advies over privacyvraagstukken en beschikt ook over een beperkte expertise op het gebied het privacy recht.

4. Rechten van betrokkenen

De gemeente dient de betrokkenen van wie zij de persoonsgegevens verwerkt zowel actief als passief te informeren over het verwerken, de wijze van het verwerken, de grondslag en de maatregelen die zij neemt om onrechtmatige toegang en - verwerking te voorkomen.
Daarnaast stelt de AVG betrokkenen in staat om door middel van een aantal rechten, controle en invloed uit te oefenen over hun eigen persoonsgegevens.
Informatie hierover staat in de privacyverklaring op de gemeentewebsite maar deze is nog niet compleet. Verder dient informatieverstrekking over specifieke verwerkingen binnen de verschillende gemeentelijke domeinen plaats te vinden via de gemeentewebsite, folders, mondeling of op andere wijze.

Verzoek rechten betrokken in 2019
Het aantal verzoeken van betrokkenen met betrekking tot het uitoefenen van hun privacy rechten bleef in het jaar 2019 beperkt tot één inzageverzoek dat betrekking had op gegevensverwerking binnen het domein openbare orde en veiligheid. Dit aantal verzoeken kan snel veranderen. Daarop moet de gemeente zijn voorbereid. Via de website van de gemeente Leusden kunnen inwoners en andere betrokkenen, konden hun verzoeken om hun rechten uit te oefenen, in 2019 nog niet online

indienen. Inmiddels is dat wel het geval. Een mooie verbetering in het veiliger kunnen verwerken van deze verzoeken.
Belangrijk is dat de processen voor de uitoefening door betrokkenen van hun privacy rechten in 2020 verder worden doorontwikkeld. Bij voorkeur geschiedt dat in BLNP-verband.

5. Samenwerking

De gemeente Leusden werkt op meerdere beleidsterreinen, in verschillende bedrijfsfuncties, in diverse rollen en hoedanigheden samen met (mede) overheden en private organisaties. In veel gevallen zal er sprake zijn van een verwerking van persoonsgegevens tussen partijen: het ontvangen van persoonsgegevens, verzenden van persoonsgegevens, maar ook het opslaan van en inzage hebben in persoonsgegevens vallen onder dit begrip. Deze verwerkingen dienen dan ook te voldoen aan de AVG.
De gemeente Leusden dient hierover afspraken te maken met deze partijen, te meer omdat de gemeente Leusden veel (uitvoerende) taken heeft uitbesteed, is van belang dat goed duidelijk is wie waarvoor verantwoordelijk is. In het geval van incidenten met betrekking tot persoonsgegevens of anderszins zou dit anders kunnen leiden tot situaties waarin de gemeente wel verantwoordelijk is maar geen zeggenschap uitoefent over de wijze waarop met persoonsgegevens wordt omgegaan. Dit kan leiden tot onveilige opslag en onveilig gebruik van persoonsgegevens en hierdoor ongewenste situaties voor de betrokkenen, kosten en imagoverlies aan de kant van de gemeente.

6. Beveiliging

Vanuit het algemene behoorlijkheidsbeginsel, het integriteitsbeginsel en het vertrouwelijkheids-beginsel is het essentieel dat de gemeente Leusdenpassende technische en organisatorische maatregelen neemt ter beveiliging van persoonsgegevens. Vanwege de bedrijfsvoering samenwerking, is van belang dat de BLNP gemeenten zoveel mogelijk uniforme maatregelen treffen, met lokaal maatwerk waar dat nodig is. De BLNP CISO en de lokale CISO's zien hierop toe in het kader van de Baseline Informatieveiligheid Overheden (BIO). Daarnaast geldt onder de AVG een meldplicht datalekken. Deze houdt in dat incidenten ten aanzien van de beveiliging –waaronder inbreuken met persoonsgegevens– onder bepaalde omstandigheden gemeld dienen te worden aan de AP en soms ook aan de betrokkene(n).

De samenwerking tussen BLNP-CISO, lokale CISO, privacy beheerder, informatie-adviseur en FG was, in 2019, binnen de beperkte capaciteit die er soms was, goed. Bij incidenten wisten zij elkaar goed te vinden maar voor cruciale taken in preventieve zin, zoals het al bij het ontwerp rekening houden met beveiliging van persoonsgegevens (privacy by design) en het treffen van standaardvoorzieningen om deze gegevens te kunnen beschermen (privacy by default), werd nog te weinig toegekomen. Aanpassen van werkprocessen of aanschaf van nieuwe systemen gebeurt nog te veel buiten het BLNP brede en buiten het lokale team voor Informatisering vraagstukken om. Nieuwe systemen en andere "tools" met impact op persoonsgegevens worden vaak langs andere kanalen aangeschaft. Informatiemanagement is nog niet afdoende gepositioneerd binnen BLNP terwijl dit het portaal zou moeten zijn waar aanvragen voor nieuwe systemen, incl. de privacy aspecten, worden beoordeeld. Hierdoor kunnen er later eventueel nieuwe investeringen en aanpassingen nodig zijn.

Daarnaast is privacybescherming maar deels een informatisering- of juridisch vraagstuk. Het betreft evenzeer bestuurlijk (ethische), beleidsontwikkelings- en control taken. Dit zijn terreinen waarbinnen

privacy bewustwording nog moet groeien. Deze situatie bemoeilijkt de borging van een veilige werkwijze. Een gestructureerde aanpak, onder meer door het hanteren van een Privacy PDCA cyclus (Plan Do Check Act) is daarom noodzakelijk en ook vereist in het kader van zowel de BIO.

Aantallen incidenten met persoonsgegevens in 2019
Er waren binnen de gemeente Leusden in 2019 in totaal 13 incidenten met persoonsgegevens, waarvan er 2 gemeld zijn aan de Autoriteit Persoonsgegevens en 2 ook gemeld zijn aan de betrokkene op wie de gelekte gegevens betrekking hadden. Dit betrof vanuit de gemeente zelf geen incidenten met grote impact maar voornamelijk verkeerd geadresseerde of bezorgde brieven, of verkeerd geadresseerde email. Ook hiervoor kan een grote impact voor de betrokkene niet helemaal worden uitgesloten. Bij de afhandeling van één van de verkeerd geadresseerde brieven bleek er onduidelijkheid te zijn over de positie van de gemeente en de gemandateerde externe partij die de brief had geadresseerd. Hierover loopt nog een nader onderzoek. In één geval ging het om diefstal van een informatiedrager met persoonsgegevens door een auto inbraak. Verklaard is dat dit geen gevoelige persoonsgegevens betrof.

Eén incident waarbij de gemeente Leusden via een andere instantie was betrokken was zeer ernstig en leidde zelfs tot Kamervragen over de toedracht: het incident waarbij via de gecertificeerde instelling Samen Veilig Midden Nederland (SVMN), zeer gevoelige persoonsgegevens met betrekking tot kinderen via klokkenluiders terecht kwamen bij RTL Nieuws. Dit datalek is inmiddels gedicht. Binnen de gemeente Leusden wordt de vrijwillige jeugdhulpverlening uitgevoerd door Stichting Lariks. De drang en gedwongen hulpverlening is via een aanbestedingsprocedure bij Samen Veilig Midden Nederland belegd en wordt uitgevoerd door het SAVE team Amersfoort. De persoonsgegevens die SAVE team Amersfoort verwerkt van inwoners van de gemeente Leusden bij drang en gedwongen hulpverlening op basis van de Jeugdwet vallen onder de verwerkingsverantwoordelijkheid van dit team. Het belang van een goede gemeentelijke regie op uitbestede verantwoordelijkheden en samenwerking bij gedeelde verantwoordelijkheden met betrekking tot persoonsgegevens van (kwetsbare) inwoners wordt door dit voorval wel onderstreept.

Een overzicht van de incidenten met persoonsgegevens in 2019 binnen de gemeente Leusden vindt u in bijlage 2 bij deze rapportage.

7. Verantwoording

De AVG legt de verantwoordelijkheid bij de organisatie zelf om aantoonbaar te maken dat deze voldoet aan de privacyregels. Door te voldoen aan de verantwoordingsplicht, levert de organisatie een belangrijke bijdrage aan de bescherming van het grondrecht van mensen op privacy. Dit betekent dat zowel de raad als het college moet kunnen aantonen dat het door hen gevoerde beleid ten aanzien van de verwerkingen van persoonsgegevens voldoet aan de beginselen van de AVG en aan de relevante wet- en regelgeving.

Het afleggen van verantwoording over de verwerking van persoonsgegevens geschiedde in Leusden in 2019 voornamelijk via de privacyverklaring op de gemeentewebsite en het daarin opgenomen register van verwerkingsactiviteiten, zie:
https://www.leusden.nl/fileadmin/user_upload/Bestanden/Documenten/Over_deze_website/Def.register-Leusden_17072018_publicatieversie_v1.0.pdf

Een DPIA- overzicht ontbrak nog in 2019, evenals andere rapportages in het kader van privacy monitoring. Verplichte controles ten aanzien van de informatiebeveiliging, inclusief de beveiliging van persoonsgegevens zijn uitgevoerd, zoals de verplichte controles ten aanzien van de informatiebeveiliging, waaronder de ENSIA audit op DigiD en Suwinet, waarover de gemeenteraad jaarlijks wordt geïnformeerd.

8. Conclusie

In 2019 is zowel binnen de bedrijfsvoering samenwerking BLNP, als lokaal door de privacy beheerder en de CISO met de andere privacybeheerders, CISO's en FG heel wat werk verzet om de AVG verder te kunnen implementeren in de organisatie en in te spelen op incidenten die een inbreuk gaven op de persoonsgegevens. De effectiviteit van privacybescherming valt of staat met de bereidheid van de organisatie om hierin verder te willen investeren in het in het belang van inwoners, bestuurders, medewerkers en mensen uit organisaties waarmee wordt samen gewerkt.

Wanneer voor de FG-taken een FG voor meerdere gemeenten tegelijk wordt ingezet, is voldoende medewerking bij het kunnen uitvoeren van deze wettelijke taak onontbeerlijk.

Gemeente Leusden

Deel 2. Vooruitkijken naar 2020 en daarna

Gegevensbescherming onderdeel laten worden van de organisatie, en daarmee aantoonbaar voldoen aan de relevante wet- en regelgeving, is geen afvinklijst, maar een continu proces. Het vraagt om een structurele borging van dit onderwerp. Daartoe moet de organisatie wel bereid en in staat zijn. De organisatie is gebaat bij het meer inzetten op planmatige/programmatechnische benadering en bij structurele aandacht hiervoor binnen management/BLNP. Door het op basis van de privacygovernance verder uitwerken van het privacybeleid, het opstellen van een realistische jaarplannen, de aanschaf van een ondersteunend systeem (ISMS) kan hieraan verder vorm en inhoud worden gegeven.

Na eerder gewerkt te hebben aan het voldoen aan de minimaal vereiste wettelijke verplichtingen die de AVG stelt, zoals het aanmelden van een Functionaris Gegevensbescherming bij de Autoriteit Persoonsgegevens, het transparant maken van hoe de gemeente omgaat met persoonsgegevens (privacyverklaring op de gemeentewebsite) en het bijhouden van een register van verwerkingsactiviteiten (ook te vinden op de gemeentewebsite) is in 2019 gewerkt aan de verdere implementatie van de AVG en getracht om de organisatie daarin verdere stappen te laten zetten. Dit gebeurde in BLNP verband en lokaal.

Het doel is om de organisatie in 2020 en daarna daar verder in mee te krijgen om daardoor aantoonbaar beter te kunnen voldoen aan deze wet. Dit vraagt om meer te investeren in de bescherming van persoonsgegevens in BLNP-verband en lokaal, binnen alle gemeentelijke domeinen. Dit gebeurt onder de verantwoordelijkheid van de betrokken bestuursorganen en wat betreft de uitvoeringspraktijk, onder die van daarvoor nog aan te wijzen proceseigenaren binnen de domeinen. Aandachtspunt daarbij is dat duidelijk moet zijn wat vanuit het BLNP samenwerkingsverband wordt opgepakt en wat vanuit de gemeente Leusden zelf.

Aanbevelingen FG voor 2020 en daarna

Puntsgewijs volgen hierna de voornaamste aanbevelingen voor onderdelen Privacy beleid en Organisatorische inbedding uit Deel 1, de Terugblik.

1. Privacybeleid

Algemeen privacy beleid en -deelbeleid

Aanbeveling 1: Richt de privacygovernance verder in, werk het algemeen Privacy beleid verder uit, werk deelbeleid uit en implementeer het beleid.

Om verder te kunnen groeien in privacyvolwassenheid dan niveau 1-3, zoals nu het geval is (zie figuur hieronder), dient het algemeen privacy beleid, na de vaststelling hiervan door het college, door het management te worden geïmplementeerd in de vele werkprocessen waarbinnen de verwerking van persoonsgegevens aan de orde is.

Voorwaarde daarbij is dat de privacy governance, bijlage 1 bij het algemeen privacy beleid binnen de gemeente Leusden, verder wordt ingericht en toegepast. De coördinerend proceseigenaar privacy en de proceseigenaren voor de andere domeinen: bestuur, sociaal domein, ruimte, openbare orde en veiligheid, publieksdiensten en ondersteuning dienen nog te worden aangewezen, evenals aandacht functionarissen binnen de teams en anderen met een rol binnen de privacy governance om samen met de privacybeheerders. Op advies van de FG kunnen acties worden ingezet om privacybewustzijn verder te kunnen ontwikkelen en privacybescherming beter te kunnen borgen binnen processen, procedures, , stappenplannen/informatiemateriaal en contacten met betrokkenen (burgers, medewerkers, partijen waarmee de gemeenten samenwerkt).

Strategisch: <u>Vooral college(s):</u> als eigenaar van de gemeentelijke informatieprocessen en (informatie)systemen een passend niveau van informatieveiligheid en privacybescherming bevorderen.

FG-taak: informeren organisaties, inwoners, medewerkers, derden, advies aan colleges (o.a. eindadvies n.a.v. datalekken), intern toezicht op naleving van de AVG en aanverwante wetgeving, aanspreekpunt extern toezichthouder (Autoriteit Persoonsgegevens), inwoners, medewerkers, derden

Tactisch: <u>Vooral management:</u> Acties die volgen uit het privacy beleid prioriteren (regiegroep/proceseigenaren/privacybeheerders)

FG-taak: advies aan en -waar nodig- overleg met regiegroep/secretarissen/proceseigenaren privacy

Operationeel: Vooral proceseigenaren privacy, ondersteund door de privacybeheerders: Uitvoering van het Privacy jaarplan (waar nodig met advies van FG)

Aanbeveling 2: Laat het management werken aan privacy bewustzijn en het actief uitdragen van het privacy beleid.
Het beleid moet door het management bekrachtigd worden en actief worden uitgedragen. Er dient (in BLNP verband) een communicatievorm te worden bepaald waarmee binnen de organisaties en in

een geschikte vorm ook buiten de organisatie het beleid kenbaar kan worden gemaakt. Regiegroep, coördinerend proceseigenaren, privacybeheerders, BLNP CISO en lokale CISO team communicatie BLNP en de FG dienen af te stemmen hoe dit gebeurt en welke communicatiemiddelen daarbij worden ingezet, zoals internet, intranet, informatiebijeenkomsten etc.

2. Organisatorische inbedding

Naast het vaststellen en inrichten van privacybeleid/governance en het werken aan privacybewustwording (training/opleiding) is het nodig om daadwerkelijk op privacybescherming te sturen door het toepassen van risicomanagement. Dit gebeurt door vanaf het begin van processen, privacy by design (door ontwerp) en privacy by default (privacy als standaardinstelling) door te voeren, door de voortgang cyclisch te monitoren en door -waar nodig- tijdig te anticiperen en inteveniëren.

ISMS

Aanbeveling 3: Bepaal -in BLNP verband- welk (verplicht) ISMS wordt aangeschaft
In het kader van de BIO zijn overheden verplicht om een ISMS te hanteren. In het kader van de AVG geldt die verplichting niet maar het ISMS is geschikt voor toepassing binnen beide taakgebieden. In BLNP verband dient te worden bepaald welk system het meest geschikt is voor aanschaf in BLNP-verband om daarmee kosten te kunnen besparen voor de individuele gemeenten. Hiertoe wordt in 2020 een voorstel voorbereid vanuit het team Informatisering BLNP.

DPIA's

Aanbeveling 4: Geef prioriteit aan het inventariseren en uitvoeren van DPIA's
Laat door de privacybeheerders(s) in overleg met de betrokken proceseigenaren privacy een lijst uitwerken van de processen en applicaties waarvoor een DPIA moet worden opgemaakt, maak een (meerjaren)planning en stel deze vast, met een marge en middelen voor het (laten) uitvoeren van dringende planbare DPIA's. Houd rekening met het vereiste dat DPIA's 1 x per 3 jaar dienen plaats te vinden.

Privacy Quick Scan Sociaal Domein

Aanbeveling 5: Werk de aanbevelingen uit de Privacy Quick Scan Sociaal Domein verder uit in acties en voer deze uit

Privacyrisico's binnen verschillende domeinen

Aanbeveling 6: Bepaal hoe inzicht wordt verkregen in privacy risico's binnen verschillende domeinen
Een privacy quickscan- of privacy zelfscan kan ook binnen de overige domeinen inzicht verschaffen en vervolgens leiden tot nog noodzakelijke acties. Gezien de ontwikkelingen op het terrein van bijvoorbeeld uitwisseling van persoonsgegevens in het kader van maatregelen tegen ondermijning, datagebruik in de openbare ruimte (gebruik van sensoren, camera's, smart city projecten etc), is een goede regievoering op privacybescherming onontbeerlijk. De maatregelen met een eventuele impact op inwoners maar ook op medewerkers binnen de gemeente vanwege het coronavirus zullen in het bijzonder alertheid vragen van het domein Openbare Orde en Veiligheid maar ook van het domein Ondersteuning (HRM) en mogelijk van andere domeinen.

Positie FG, privacy beheerder en CISO's

Aanbeveling 7: zorg voor de (wettelijk verplichte) positionering, ondersteuning en faciliteiten van de FG in de organisatie. Dit geldt (hoewel niet wettelijk verplicht) ook voor de privacy beheerder en (BLNP) CISO's.

Als FG heb ik in 2018 en 2019 intensief mee gedacht en mee gebouwd aan de privacy organisatie zoals die er nu staat. Vanaf 2020 zal ik mij meer gaan richten op en meer beperken tot de wettelijk ingekaderde taken. De zorg voor de privacy organisatie behoort bij het management van de organisaties. Hierover dienen goede werkafspraken te worden gemaakt in BLNP-verband en lokaal.

Aanbeveling 8: Zorg (in BLNP-verband) voor borging van privacy recht advies voor praktijkcases

Om aan verdere borging van de AVG en aanverwante (sectorale) privacywetgeving te kunnen voldoen binnen de diverse gemeentelijke domeinen, is een ruimere investering in juridische ondersteuning met betrekking tot privacy recht advies in verband met praktijkcases noodzakelijk. Het juridisch team BLNP kan hierin maar beperkt voorzien, terwijl de FG een meer strategische adviestaak en toezichthoudende taak heeft die niet samengaat met het oplossen van praktijkcases. Omdat een gebrek aan privacy recht advies in de vier gemeenten speelt, ligt het voor de hand om de oplossing hiervoor in BLNP-verband te onderzoeken.

Gezamenlijke aanpak privacy taken in BLNP verband versus lokale aanpak

Aanbeveling 9: Bepaal wat binnen het BLNP samenwerkingsverband wordt opgepakt en wat lokaal en richt dit in.

In 2019 kon in de BLNP gemeenten aan privacybescherming binnen de diverse domeinen niet voldoende recht gedaan worden. Alles hoeft ook niet tegelijk te gebeuren, de AVG biedt ruimte om prioriteiten te stellen maar dit dient wel gestructureerd te gebeuren om een verantwoord privacy beleid te kunnen voeren. Veel zal in BLNP verband kunnen worden opgepakt en worden afgestemd met en tussen de betrokken proceseigenaren.

Behalve voor Informatisering, Juridische Zaken, Financiën en HRM is de BLNP-samenwerking voor andere taakgebieden niet geformaliseerd, terwijl privacy taken daarin doorwerken en specifieke aandacht behoeven. Onderzocht moet worden in hoeverre samenwerking in BLNP-verband wenselijk is en als dit niet wenselijk is, hoe de privacy taken die niet in BLNP verband hun beslag krijgen, lokaal dienen te worden uitgevoerd vanuit de BLNP-samenwerking.

3. Conclusie

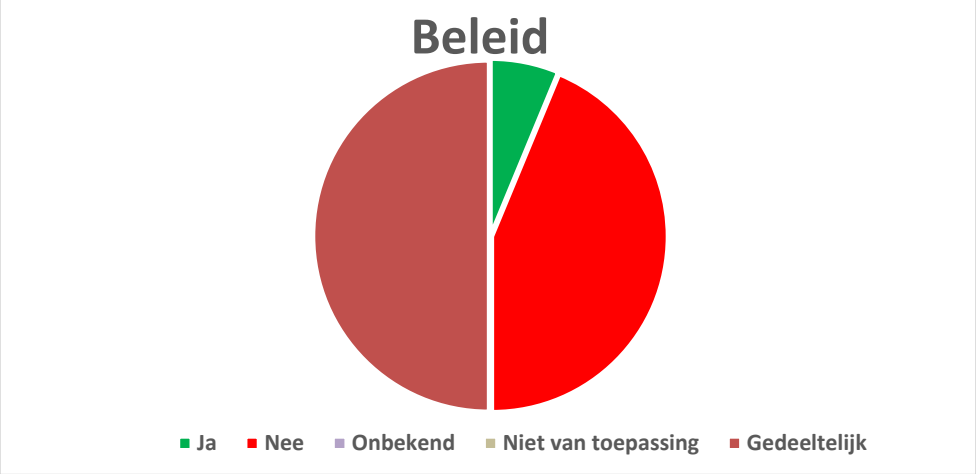
Op het gebied van privacy en gegevensbescherming is er in 2020 en daarna veel winst te behalen. Op alle niveaus werken aan privacy bewustwording, via het BLNP samenwerkingsverband en lokaal, door middel van een gestructureerde aanpak, verdient de komende tijd extra aandacht. Privacybescherming moet meer aan de voorkant van de gemeentelijke processen kunnen starten om risico's vooraf voldoende in beeld te kunnen krijgen en deze beheersbaar te kunnen houden in een tijd vol onzekerheden en verandering. De toepassing van de BIO en de AVG kan alleen slagen als deze kan worden verweven binnen de gemeentelijke domeinen.

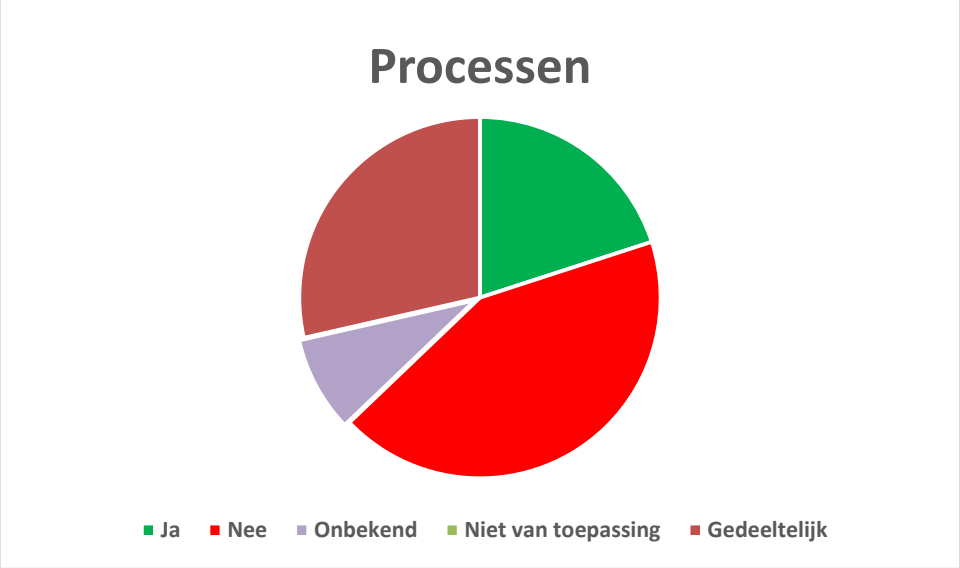
De lokale organisaties dienen te bepalen hoe zij binnen BLNP en/of lokaal invulling wensen te geven aan processen, samenwerkingsvormen en beleidsonderwerpen waar privacybescherming een wezenlijk onderdeel van uitmaakt. De regiegroep is verantwoordelijk voor vorm en inhoud van de BLNP- bedrijfsvoeringsamenwerking. Daaronder valt ook de borging van de AVG vanuit het samenwerkingsverband.
Eén en ander vraagt om een risico gestuurde aanpak omdat binnen gemeenten alles niet meer tegelijkertijd kan worden opgepakt. Het slim inzetten van intrinsiek motiverende energiebronnen, zoals het tonen van aansprekend voorbeeldgedrag, het stimuleren van en het durven nemen van voldoende autonomie, het veilig kunnen geven en ontvangen van feedback en een hulpvaardige houding naar collega's, is daarbij cruciaal. Dit vraagt een open communicatie. Obstructief gedrag moet tijdig worden onderkend en actief worden tegengegaan.

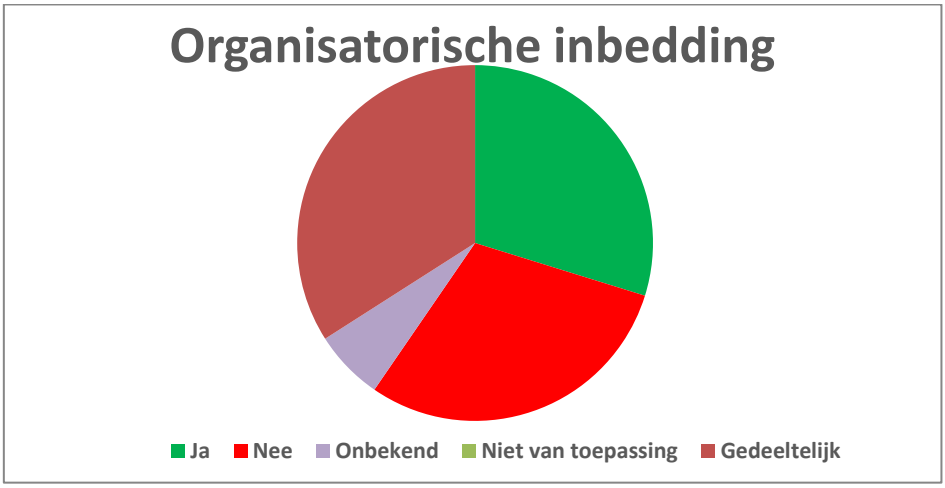
Onder deze condities kan invulling gegeven worden aan het worden van een "risicogestuurde en data gedreven gemeente" waarbinnen persoonsgegevens in veilige handen zijn.

Er zijn kortom nog aandachtspunten voor de vier organisaties om aantoonbaar te kunnen voldoen aan de AVG maar dit kan gefaseerd gebeuren en is nog steeds heel goed te realiseren in Leusden en binnen het BLNP samenwerkingsverband. Daar denk ik als FG graag bij mee.

Bijlage 1. Stand van zaken AVG per onderwerp[3]

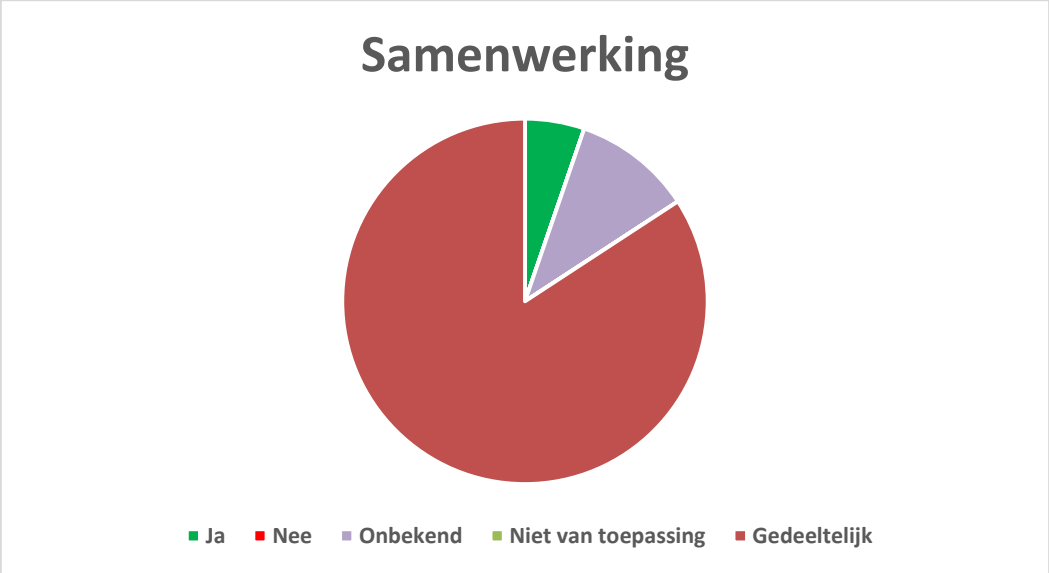






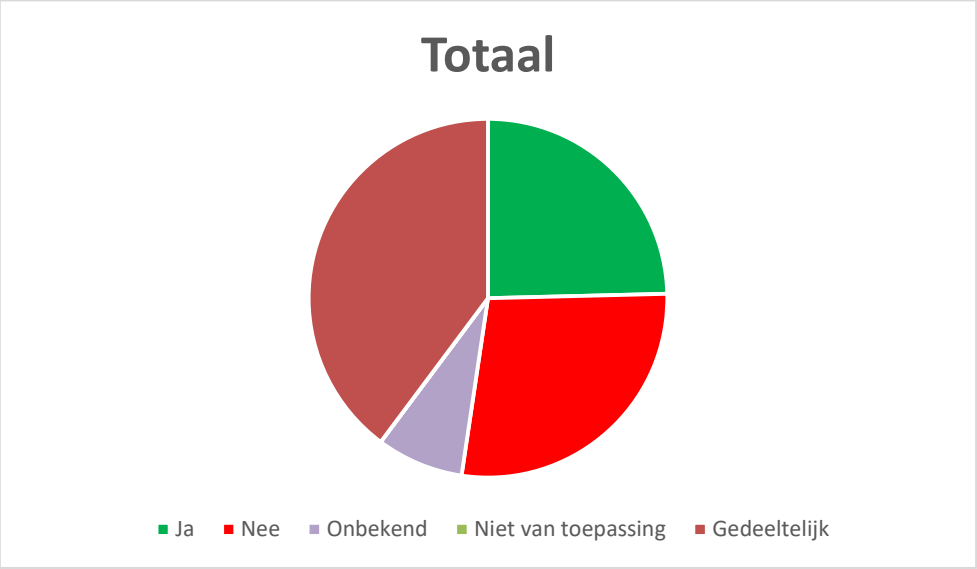
[3] Tabblad 2 van het Exceldocument tweede tabblad


Rechten van betrokkenen
Ja
Nee
Onbekend
Niet van toepassing
Gedeeltelijk


Samenwerking
Ja
Nee
Onbekend
Niet van toepassing
Gedeeltelijk


Beveiliging
Ja
Nee
Onbekend
Niet van toepassing
Gedeeltelijk


Verantwoording
Ja
Nee
Onbekend
Niet van toepassing
Gedeeltelijk


Totaal
Ja
Nee
Onbekend
Niet van toepassing
Gedeeltelijk

BIJLAGE 2 OVERZICHT VAN INCIDENTEN MET PERSOONSGEGEVENS IN LEUSDEN IN 2019

Aantal incidenten in totaal: 13	
Aantal incidenten gemeld aan de Autoriteit Persoonsgegevens: 2	**Aantal incidenten gemeld aan AP + aan de betrokkene(n): 2**
Aantal incidenten waarvoor derden verantwoordelijk zijn: 1	**Aantal incidenten waarvoor gem. Leusden verantwoordelijk is: 12**

Soort incidenten:	Aantal:
1. Persoonsgegevens die ten onrechte intern openbaar gemaakt zijn	-
2. Persoonsgegevens die ten onrechte (intern) en/of extern openbaar gemaakt zijn:	3
3. Persoonsgegevens die naar een verkeerde ontvanger gestuurd zijn:	8
4. Persoonsgegevens die verloren gegaan zijn door verlies/diefstal/kwijt raken etc. van een gegevensdrager (mobiele telefoon, laptop etc):	1
5. Persoonsgegevens die door hacking, malware, phishing bij onbevoegden terecht gekomen zijn:	-
Incidenten waarvoor derden verantwoordelijk zijn:	
Persoonsgegevens van inwoners/medewerkers die door derden gelekt zijn en waarbij de gemeente betrokken is/of kennis van gekregen heeft.	1