Afdeling: Bestuur en Dienstverlening
Behandelaar: beekman, Sascha
Telefoonnummer: **381**

Voorstelnr. 1946
Barneveld, 3 februari 2022
Portefeuillehouder: A.H. van de Burgwal

☐ Ter kennisname naar de raad
Nummer beleidsproduct:

☐ Op overzicht Bestaand beleid (website)

Onderwerp: **Jaarverslag Functionaris Gegevensbescherming 2021**

Gevraagde beslissing:
1. Het bijgevoegde Jaarverslag FG 2021 vast te stellen;
2. De memo en het Jaarverslag FG 2021 via rubriek B ter kennisname te doen toekomen aan de gemeenteraad;
3. Ter voldoening aan de verplichte registratie en publicatie het Jaarverslag FG 2021 op de website van de gemeente te plaatsen.

1. Inleiding
Op 25 mei 2018 is de Europese Algemene verordening gegevensbescherming (AVG) van toepassing geworden in de hele Europese Unie. In Nederland is op die dag de Wet bescherming Persoonsgegevens komen te vervallen. Dit jaarverslag geeft weer wat de Gemeente Barneveld in 2021 heeft ondernomen om aan de vereisten van de AVG te voldoen.

2. Beoogd effect
De bestuursorganen van de gemeente en de inwoners worden geïnformeerd over wat de Gemeente Barneveld in 2021 heeft ondernomen om aan de vereisten van de AVG te voldoen.

3. Argumenten
1.1. De rapportage geeft een goed inzicht in wat de Gemeente Barneveld in 2021 heeft ondernomen om aan de vereisten van de AVG te voldoen
In 2021 zijn de volgende zaken gerealiseerd:
- het Privacybeleid is geactualiseerd en vastgesteld;
- het register van verwerkingen is geactualiseerd;
- er zijn nieuwe of geactualiseerde verwerkersovereenkomsten afgesloten met vele verwerkers;
- er zijn intern veel adviezen gegeven en (online) workshops gehouden over privacy en informatieveiligheid;
- er zijn meerdere Data Protection Impact Assessments (DPIA) uitgevoerd, waarmee een goede risico-analyse gemaakt kan worden over hoe er per vakgebied omgegaan wordt met het verwerken van (persoons)gegevens. In 2021 is een deel van de 2018/2019 uitgevoerde DPIA's herzien, omdat de AVG vereist dat DPIA's iedere 3 jaar uitgevoerd worden. In 2022 wordt hiermee verder gegaan.

Vanwege de coronapandemie is er vanaf medio maart 2020 en in heel 2021 door de meeste medewerkers veel vanuit huis gewerkt. Thuiswerken brengt risico's met zich mee op het gebied van privacy en informatiebeveiliging, zodat daar extra aandacht voor gevraagd is in meerdere nieuwsbrieven en berichten op intranet.

2.1. Conform het Privacybeleid wordt de gemeenteraad geïnformeerd
De AVG en het Privacybeleid van de Gemeente Barneveld schrijven voor dat de FG jaarlijks voor 1 maart verslag uitbrengt aan de bestuursorganen. Het onderhavige verslag wordt dan ook uitgebracht aan het college van burgemeester en wethouders, de burgemeester en de gemeenteraad van Barneveld.

3.1 Publicatie van het jaarverslag op de website geeft openheid
Met het publiceren van het Jaarverslag FG 2021 voldoet het college aan de in de AVG en het Privacybeleid opgenomen verplichting. Hiermee geeft uw college aan de inwoners en andere belangstellenden opening van zaken over wat de Gemeente Barneveld in 2021 heeft ondernomen om aan de vereisten van de AVG te voldoen. In het verslagjaar wordt toegelicht welke werkzaamheden zijn uitgevoerd en wat de acties voor het komende jaar zijn.

4. Kanttekeningen
n.v.t.

5. Financiën
n.v.t.

6. Uitvoering
n.v.t.

7. Bijlagen
1. Jaarverslag FG 2021
2. Memo aan raad

gemeente Barneveld

Jaarverslag

Functionaris Gegevensbescherming 2021

Jaarverslag

Functionaris Gegevensbescherming 2021

Opdrachtgever:	gemeente Barneveld Afdeling Bestuur & Dienstverlening
Auteur:	Sascha Beekman, Functionaris Gegevensbescherming
Datum:	11 februari 2022

Inhoud

1. Managementsamenvatting 3
2. Wettelijk kader 5
   2.1. AVG Algemeen 5
   2.2. Specifieke wetgevende ontwikkelingen, jurisprudentie en nieuwsberichten van Autoriteit Persoonsgegevens 5
   2.3. Toezichtskader AP: ontwikkelingen en gevolgen 7
3. Governance 10
   3.1 Governance algemeen 10
   3.2 Verantwoording Functionaris gegevensbescherming 10
   3.3 Verantwoording Privacy Officer 11
   3.4 Verantwoording CISO 12
   3.5 Borging 12
   Tabel. 13
   Grafiek. 14
4. Werkzaamheden en bevindingen 15
   4.1 Privacybeleid 15
   4.2. Thuiswerken 15
   4.3. Register van verwerkingen 16
   4.4. Meldingen datalekken 16
   4.5. Rechten van betrokkenen 17
   4.6. Bewaartermijnen 17
   4.7. Verwerkers en verwerkersovereenkomsten 17
   4.8. Privacy in het Sociaal Domein 18
   4.9. Informatieveiligheid 19
   4.10. Data Protection Impact Assessments 19
   4.11. Bewustwording 21
   4.12. Overige zaken 21
5. Aanbevelingen en acties 23
   5.1. Aanbevelingen 23
   5.2. Acties voor 2022 24

1. MANAGEMENTSAMENVATTING

Op 25 mei 2018 is de Europese Algemene verordening gegevensbescherming (AVG) van toepassing geworden in de hele Europese Unie. In Nederland is op die dag de Wet bescherming Persoonsgegevens komen te vervallen. De gemeente Barneveld heeft de bescherming van de privacy van de Barneveldse inwoners en het verwerken van de (persoons)gegevens van deze inwoners met de komst van de AVG opnieuw beoordeeld en waar nodig verbeterd.

Dit jaarverslag – dat mede in samenwerking met de Privacy Officer (PO) en de Chief Information Security Officer (CISO) – door de Functionaris Gegevensbescherming (FG) is opgesteld, geeft weer wat de Gemeente Barneveld in 2021 heeft ondernomen om aan de vereisten van de AVG te voldoen.

Het register van verwerkingen is geactualiseerd, er zijn nieuwe of geactualiseerde verwerkersovereenkomsten afgesloten met vele verwerkers. Ook zijn er intern veel adviezen gegeven en (online) workshops gehouden over privacy en informatieveiligheid, omdat deze onlosmakelijk met elkaar verbonden zijn en het belangrijk is dat het bewustzijn bij de medewerkers aanwezig is en dat ook blijft. Daarbij is niet alleen aandacht besteed aan de grondslag en doelbinding die aanwezig moet zijn voordat gegevens verwerkt mogen worden, welke gegevens verwerkt mogen worden en hoe lang deze bewaard mogen worden, maar ook is het belang onderstreept van een zorgvuldige verwerking en deling van gegevens door bijvoorbeeld gebruik te maken van beveiligd e-mailen.

Vanwege de coronapandemie is er vanaf medio maart 2020 door de meeste medewerkers veel vanuit huis gewerkt. Thuiswerken brengt nieuwe mogelikheden, maar ook risico’s met zich mee op het gebied van privacy en informatiebeveiliging, zodat daar extra aandacht voor gevraagd is in meerdere nieuwsbrieven en berichten op intranet.

De aanbevelingen en de – waar nodig – te nemen maatregelen voortkomend uit de rapportages over de in 2020 uitgevoerde Data Protection Impact Assessments (DPIA’s), waarmee een goede risico-analyse gemaakt is over hoe er per vakgebied omgegaan wordt met het verwerken van (persoons)gegevens, zijn in 2021 geëvalueerd en beoordeeld op aanpak en uitvoering. In 2022 komt daar een vervolg op en zullen eveneens een aantal nieuwe en herziene DPIA’s uitgevoerd worden.

De gemeente Barneveld heeft de bescherming van privacy en een goede informatieveiligheid hoog in het vaandel staan. Veel is goed geregeld. Om dit zo te houden, dient er continue aandacht besteed te worden aan privacy van burgers, bedrijven en medewerkers, waarbij een zorgvuldige verwerking van de persoonsgegevens en de bescherming daarvan steeds gewaarborgd moet zijn. Het jaar 2021 stond, evenals 2020, in het teken van borging, waarbij de verwerking van persoonsgegevens en de bescherming daarvan nog beter verankerd zal worden in de organisatie door middel van protocollen, procedures, bewustzijnsacties, waar nodig

aanpassingen in applicaties en software, en dat de medewerkers zich daarvan bewust zijn en ook daarnaar handelen.

Daarnaast is in 2021 aandacht besteed aan de evaluatie van de eerder gecommuniceerde aanbevelingen en te nemen maatregelen om de verwerking van persoonsgegevens en onder andere de bewaartermijnen beter te borgen en na te leven. Ook is het privacybeleid herzien. In 2021 is er een evaluatie gestart over het gebruik van cameratoezicht in het centrum van Barneveld. Zodra de resultaten van de evaluatie bekend zijn, wordt in 2022 bepaald of inzet van cameratoezicht noodzakelijk is en voortgezet wordt. Als cameratoezicht blijvend ingezet gaat worden, wordt daarvoor camerabeleid opgesteld, waarbij de mogelijkheden en risico's voor privacy en informatiebeveiliging goed tegen elkaar afgewogen moeten worden.

2. WETTELIJK KADER

2.1. AVG Algemeen

In de Algemene Verordening Gegevensbescherming (AVG) zijn regels vastgelegd voor het verwerken van persoonsgegevens. Deze verordening voor de verwerking van persoonsgegevens kent een rechtstreekse werking voor de lidstaten van de Europese Unie. In de AVG worden de rechten van burgers versterkt en de AVG legt de nadruk op de eigen verantwoordingsplicht van organisaties die persoonsgegevens verwerken. Dit betekent dat organisaties bijvoorbeeld goed moeten vastleggen welke gegevens zij verwerken, met welk doel, hoe lang zij die gegevens bewaren, dat zij de gegevens goed beveiligen en met wie ze gegevens delen. De rechtstreekse werking van de AVG zorgt ervoor dat de regels voor bescherming van persoonsgegevens uniform zijn binnen de Europese Unie.

De AVG geeft een overkoepelend kader voor het verwerken van persoonsgegevens en is nader uitgewerkt in de Nederlandse Uitvoeringswet AVG. Daarnaast zijn er in materiewetgeving, zoals de Jeugdwet, de Wet maatschappelijke ondersteuning, de Wet Basisregistratie personen specifieke regels te vinden voor het verwerken van persoonsgegevens. De AVG hangt daar altijd als een paraplu boven. Dat betekent dat als persoonsgegevens verwerkt mogen worden op grond van de materiewetgeving, de bepalingen van de AVG daar boven blijven hangen. Er moet bijvoorbeeld altijd een rechtmatige grondslag zijn voor het verwerken van persoonsgegevens en persoonsgegevens mogen alleen worden verwerkt voor het doel waarvoor ze zijn verzameld.

2.2. Specifieke wetgevende ontwikkelingen, jurisprudentie en nieuwsberichten van Autoriteit Persoonsgegevens

1. AP nieuwsbericht 6 mei 2021

AP verzwaart toezicht op gemeente

De AP heeft besloten het toezicht op een gemeente te verzwaren. De AP heeft zorgen of deze gemeente de (gevoelige) gegevens van de inwoners wel voldoende beschermt. De betreffende gemeente wordt daarom verplicht elke 3 maanden een uitgebreide rapportage aan de AP te verstrekken. Aanleiding zijn signalen over overtredingen van de privacywet. Verder constateert de lokale Rekenkamer dat er na dik 2 jaar AVG nog geen privacybeleid was vastgesteld. Ook stelt het rapport van de Rekenkamer dat de zowel de onafhankelijkheid als de informatiepositie van de interne toezichthouder, de functionaris gegevensbescherming (FG), onvoldoende waren geborgd. De wet verbindt duidelijke eisen aan de positionering van een FG. Zo is het essentieel dat de FG onafhankelijk kan toezien op de naleving van de AVG in de betreffende organisatie.

Verzwaren van toezicht
Het is de bevoegdheid van een inspectie of een toezichthouder te bepalen welke vorm en welke intensiteit van toezicht noodzakelijk is. Om de (gevoelige) informatie van inwoners te beschermen, is snelheid essentieel. Daarom is besloten voor een interventie die direct ingezet kan worden; het verzwaren van het toezicht. De AP heeft de gemeente gesommeerd om een jaar lang elk kwartaal een voortgangsrapportage te sturen over de maatregelen die de gemeente neemt om aan de AVG te voldoen. Het doel is dat de gemeente zorgdraagt voor een veilige en betrouwbare verwerking van persoonsgegevens van de inwoners van deze gemeente. De AP sluit een nader onderzoek niet uit. Dat kost echter veel tijd. Inmiddels heeft de gemeente de eerste rapportage aangeleverd.

Intern toezicht verplicht
Een gemeente is verantwoordelijk voor het opstellen en het uitvoeren van het privacybeleid. Net als alle overheden is een gemeente verplicht om een FG aan te stellen; een onafhankelijke, interne privacy-functionaris. De FG ziet toe op de naleving van het privacybeleid en adviseert over privacyrisico's. Voorkomen is beter dan genezen. Daarom moet de FG in een vroeg stadium betrokken worden en toegang hebben tot alle relevante informatie. Op die manier wordt de organisatie in staat gesteld maatregelen te nemen en de persoonsgegevens van burgers en klanten te beschermen.

2. AP nieuwsbericht van 30 juli 2021

AP publiceert aanbevelingen voor smart cities
De Autoriteit Persoonsgegevens (AP) publiceert aanbevelingen voor de ontwikkeling van zogenoemde smart city-toepassingen. De aanbevelingen zijn bedoeld voor gemeenten die met slimme sensoren en meetapparatuur data in de openbare ruimte verzamelen of dat van plan zijn. De adviezen van de AP zijn nodig omdat gemeenten niet altijd voldoende stilstaan bij de privacywetgeving terwijl dit juist bij smart city-toepassingen waarbij persoonsgegevens van de burgers verwerkt worden essentieel is. Slecht ontwikkelde toepassingen kunnen namelijk ten koste gaan van de vrijheid van inwoners en bezoekers van die gemeente. Bijvoorbeeld wanneer burgers in de openbare ruimte worden gevolgd op een manier die niet nodig is of niet is toegestaan. Een gemeente die technologie inzet, kan daarbij persoonsgegevens verwerken. Met sensoren of meetapparatuur worden bijvoorbeeld verkeersstromen en bezoekersaantallen gemeten of uitgaansgebieden gemonitord om de mobiliteit en veiligheid te verbeteren. De privacywet - de Algemene verordening gegevensbescherming (AVG) - beschermt mensen tegen het onnodig of ongeoorloofd verzamelen of gebruiken van hun persoonsgegevens in de openbare ruimte.

Ongedwongen over straat
Monique Verdier, vicevoorzitter AP: "*Het gevaar bestaat dat we naar een surveillancemaatschappij gaan waar je niet meer ongedwongen over straat kunt lopen. De inzet van technologie kan gemeenten weliswaar meer inzicht geven in het gebruik van de openbare ruimte, maar dat mag niet zonder stil te staan bij de prijs die*

de inwoners en bezoekers van die gemeente hiervoor betalen. Hoe verhoudt het verzamelen van hun gegevens in de openbare ruimte zich tot hun vrijheid? Wie kan er allemaal bij die gegevens en waar mogen die voor worden gebruikt? Welke informatie mag aan elkaar worden gekoppeld? De technische mogelijkheden zijn oneindig, maar aan wat ethisch en juridisch toelaatbaar is zit een grens.
Technologie kan ons helpen om onze problemen op te lossen en de stad leefbaarder en veiliger te maken. Maar we moeten het wel zo inregelen dat ze niet zelf allerlei nieuwe problemen en onveiligheidsgevoelens veroorzaken. Bestuurders en ambtenaren moeten de rechten en vrijheden van burgers uiterst serieus nemen. Dat betekent dat zij hun privacy ook daadwerkelijk meenemen bij elke stap in de ontwikkeling naar een smart city. Laat privacy het startpunt zijn van innovatie, niet het sluitstuk."

3. AP nieuwsbericht van 16 september 2021

Handreiking Wet gemeentelijke schuldhulpverlening
De gewijzigde Wet gemeentelijke schuldhulpverlening (Wgs) geeft meer duidelijkheid over wat wel en niet mag bij de verwerking van persoonsgegevens voor (de toeleiding naar) schuldhulpverlening. Toch blijken er in de praktijk nog veel vragen te zijn. Daarom heeft de Autoriteit Persoonsgegevens (AP) een handreiking opgesteld met aandachtspunten. Hiermee moeten gemeenten en hulpverleners rekening houden om aan de privacywetgeving te voldoen. De Wgs regelt dat mensen met (dreigende) problematische schulden bij gemeenten terecht kunnen voor onder meer advies, schuldbemiddeling of een saneringskrediet.

Wat is het probleem?
De AP heeft de afgelopen jaren meerdere signalen, klachten en vragen ontvangen over schuldhulpverlening. Probleem is vaak dat niet duidelijk is welke gegevens de verschillende partijen met elkaar mogen delen en onder welke voorwaarden. En dat in de praktijk gegevens worden gedeeld zonder dat daarvoor een wettelijke grondslag bestaat.
Een aantal van deze onduidelijkheden komt aan bod in de wijziging van de Wgs, die op 1 januari 2021 van kracht is geworden.

2.3. Toezichtskader AP: ontwikkelingen en gevolgen

De Autoriteit Persoonsgegevens (AP) heeft in november 2019 haar toezichtkader voor de jaren 2020 tot en met 2023 gepubliceerd. In dit kader geeft de AP haar prioriteiten aan voor de komende jaren.

De Autoriteit Persoonsgegevens (AP) legt de komende jaren in het toezichtwerk extra nadruk op drie focusgebieden: datahandel, digitale overheid en artificiële intelligentie en algoritmes. Dat maakt de AP op 11 november 2019 bekend met het visiedocument 'Dataprotectie in een digitale samenleving'. Extra nadruk op deze thema's is nodig om de bescherming van persoonsgegevens in Nederland te borgen. Misbruik of onverantwoordelijk gebruik van persoonsgegevens kan bijvoorbeeld leiden tot foutieve

beslissingen, uitsluiting van mensen en discriminatie. Tot en met 2023 geven de focusgebieden onder meer richting aan de uitvoering van de wettelijke taken van de AP.

Voorzitter Aleid Wolfsen: *"Bescherming van persoonsgegevens is een belangrijk grondrecht dat er is om ons tegen misbruik te beschermen. Het gaat in de kern over zeggenschap, over autonomie, over dat wij als burgers zelf gaan over wat we met wie delen. Ik hoor nog veel te vaak onterecht dat de privacywet ontwikkelingen in de weg staat. Het is geen kwestie van of-of, maar van en-en. Zorgvuldig omgaan met persoonsgegevens is onderdeel van ontwikkeling en innovatie."*

Trends en ontwikkelingen
Steeds meer apparaten en diensten verzamelen persoonsgegevens waardoor ze steeds meer van ons weten. Dit gebeurt zonder dat we altijd precies weten wat er met die gegevens gebeurt en wie er toegang toe heeft. Dit maakt ons en onze democratische rechtstaat kwetsbaar.

De AP ziet drie grote trends die van invloed zijn op de bescherming van persoonsgegevens:

- Doorgroei van de datasamenleving
- Toename van digitaal onrecht
- Toename van privacybewustzijn

Focusgebieden
In vervolg op de gesignaleerde trends kiest de AP voor drie focusgebieden:

Datahandel
Data maken producten en diensten slimmer en deze producten en diensten creëren vervolgens weer meer data. Dit heeft voordelen, maar ook nadelen: er vindt steeds meer ongeoorloofde doorverkoop plaats van persoonsgegevens aan derden. Mensen verliezen hierdoor steeds meer grip op hun gegevens en daarmee op hun leven.

Digitale overheid
Centrale en lokale overheden, uitvoeringsorganisaties en politie en justitie beschikken over een grote hoeveelheid – vaak gevoelige en bijzondere – persoonsgegevens. De overheid werkt gericht aan het inzetten van persoonsgegevens. Het is van belang dat de overheid verantwoordelijk omgaat met persoonsgegevens, zodat mensen niet onnodig in de knel kunnen komen.

Artificiële Intelligentie en algoritmes
Steeds meer bedrijven en organisaties maken gebruik van algoritmes en AI. Dit biedt voordelen en leidt tot nieuwe nuttige toepassingen. Maar de inzet van AI en algoritmes kent ook risico´s en schadelijke effecten. Onverantwoordelijk gebruik van algoritmes kan leiden tot foutieve beslissingen, tot uitsluiting van mensen en tot discriminatie. De AP is als toezichthouder verantwoordelijk voor het toezicht op de

verwerking van persoonsgegevens, en daarmee ook op de toepassing van AI en algoritmes waarbij persoonsgegevens worden gebruikt.

Deze thema's passen bij de missie van de AP en spelen in meerdere sectoren. De AP kan hier het verschil maken door grenzen te markeren ten aanzien van wat er wel en niet kan onder de AVG. De focusgebieden geven onder meer richting aan de uitvoering van de wettelijke taken van de AP. Daarnaast houdt de AP oog voor actuele ontwikkelingen.

Risicogestuurd toezicht

De AP is de onafhankelijke toezichthouder in Nederland die de bescherming van persoonsgegevens bevordert en bewaakt. Het toezichtveld is omvangrijk: internationale en nationale bedrijven en organisaties, de gehele overheid, inclusief politie en justitie en ook verenigingen, scholen, stichtingen en individuele burgers.

De AP houdt daarom risicogestuurd toezicht. Dat betekent dat de AP is gespitst op onderwerpen met een groot risico voor burgers. Daarbij weegt de AP af om hoeveel data het gaat en hoe gevoelig die data zijn. Op basis daarvan gebruikt de AP een of meerdere toezichtsinstrumenten, zoals normuitleg, wetgevingsadvies, voorlichting of handhaving.

3. GOVERNANCE

3.1 Governance algemeen

Er is een duidelijke structuur aangaande de governance aanwezig wat betreft de uitvoering van de AVG. Er zijn een (interim) Chief Information Security Officer (CISO), een Privacy Officer (PO) en een Functionaris Gegevensbescherming (FG) aangewezen door het college. Deze onderlinge relaties en verantwoordingen blijken uit het door het college vastgestelde en op 1 april 2018 in werking getreden Privacybeleid. Dit beleid is in 2021 herzien, op 11 mei 2021 door het college vastgesteld en op 1 juni 2021 in werking getreden. Hiermee wordt voldaan aan artikel 5 lid 2 van de AVG dat bepaalt dat een organisatie dient aan te kunnen tonen 'in control' te zijn aangaande de uitvoering van de AVG.

3.2 Verantwoording Functionaris gegevensbescherming

Overzicht uitgevoerde werkzaamheden in 2021:

In 2021 zijn er enkele Data Protection Impact Assessments (DPIA's) uitgevoerd die herzien moesten worden of vanwege aanschaf of uitbreiding van een applicatie. De rapportages van deze DPIA's worden begin 2022 afgerond, zodat het tweede en derde kwartaal van 2022 gebruikt kunnen worden om de uit de DPIA's voortvloeiende acties op te pakken en uit te voeren.

Het Register van Verwerkingen is in 2021 geactualiseerd.

In het voorjaar van 2021 is het borgingsdocument dat VNG en IBD hebben ontwikkeld, herzien en anders vormgegeven. Begin december 2021 is aan de hand van dit nieuwe document de borging beoordeeld en zijn de resultaten geëvalueerd ten opzichte van het jaar daarvoor. De daaruit voortkomende acties worden in 2022 opgepakt. Zie verder bij 3.5.

Door het vele thuiswerken vanwege de coronapandemie is er meerdere keren extra aandacht gevraagd voor privacy en informatiebeveiliging in nieuwsbrieven en intranet berichten. Dit heeft er eveneens voor gezorgd dat de "Handreiking training Informatieveiligheid en Privacy" is geactualiseerd, zodat deze herziene versie gebruikt kan worden bij de workshops voor nieuwe medewerkers.

3.3 Verantwoording Privacy Officer

Overzicht uitgevoerde werkzaamheden in 2021:

PIA's uitvoeren	In 2021 zijn een aantal DPIA's uitgevoerd op risicovolle processen, waaronder cameratoezicht bij de gemeentelijke gebouwen en de Suite4SocialeRegie.
Overige vereisten uit de AVG invoeren	Privacy by design en default zijn vanaf mei 2018 bij nieuwe applicaties als eis meegenomen. Dit wordt onder meer vormgegeven door deelname aan het Planatelier en het pro- actief handelen van collega's door de PO vroegtijdig te betrekken.
Bewustwording privacy en informatiebeveiliging	- Er zijn digitale workshops voor (nieuwe) medewerkers verzorgd. - Op verzoek zijn de CISO en/ of PO bij teamoverleggen en overleggen met leveranciers aanwezig geweest. - Periodiek is een nieuwsbericht op intranet gezet.
Privacy en Publiekszaken	In overleg met Publiekszaken is ondersteuning geboden bij privacyvraagstukken (verstrekken gegevens uit het BRP en terugmelding BRP).
Instellen + vullen register van verwerkingen	Nieuwe processen worden toegevoegd en wijzigingen in processen worden in het register doorgevoerd. Daarnaast zijn de bewaartermijnen in het register aangevuld.
Ondersteunen bij ontwikkelingen dienstverlening	Bij het ontwikkelen van nieuwe / andere vormen van de dienstverlening van Barneveld is de privacyregelgeving meegenomen en neemt waar nodig de PO deel aan (implementatie) projecten.
Privacy en Sociaal domein	Het Sociaal Domein heeft meerdere verzoeken tot recht van inzage gekregen en deze zijn samen met de betrokken gespreksvoerder en de Privacy Officer afgehandeld.
Inrichten intranet	Algemene informatie over privacy, informatiebeveiliging en werkinstructies zijn op intranet geplaatst.
Proces omtrent datalekken inregelen en monitoren	Inbreuken in verband met privacy zijn geregistreerd. Datalekken zijn gemeld bij de AP.
Instellen PO	Op 1 april 2021 is er een vaste PO aangesteld voor 24 uur per week. De PO heeft uitvoering gegeven aan: - Toetsen / opstellen verwerkersovereenkomsten - Toetsen/ opstellen convenanten - Verbeteringsslag register van verwerkingen - Uitvoeren DPIA's - Behandelen privacy vraagstukken - Signaleringsfunctie in organisatie - Sparringspartner voor de organisatie

3.4 Verantwoording CISO

Overzicht uitgevoerde werkzaamheden in 2021:

Bewustwording privacy en informatiebeveiliging	- Samen met de PO zijn workshops voor medewerkers verzorgd. - Op verzoek zijn de CISO of PO bij teamoverleggen aanwezig geweest. - De CISO neemt periodiek deel aan afdelingsoverleggen binnen I&A - Met campagnemateriaal is bewustwording gecreëerd. - Periodiek is een nieuwsbericht op intranet gezet.
Zelfevaluatie BRP/PNIK	Ieder jaar draagt de Gemeente Barneveld een verantwoording af over BRP / PNIK wetgevingen.
Zelfevaluatie ENSIA	Ieder jaar draagt de Gemeente Barneveld een verantwoording af over informatiebeveiliging door middel van ENSIA (Eenduidig Normatiek Single Information Audit). Hierin vallen ondermeer BAG, BGT, DigiD, Suwinet en BIG. Sinds 2018 valt daaronder ook de verantwoording over AVG. Daarbij worden DigiD, Suwinet en ENSIA overall getoetst door een RE/RA auditor.
BIO	Controleren en evalueren van de huidige set maatregelen.
Pentests	Er zijn (voornamelijk IT-gerichte) penetratietests uitgevoerd. De uitkomsten daarvan zijn verwerkt in veranderingen, projecten en gebruik van nieuwe tooling.

3.5 Borging

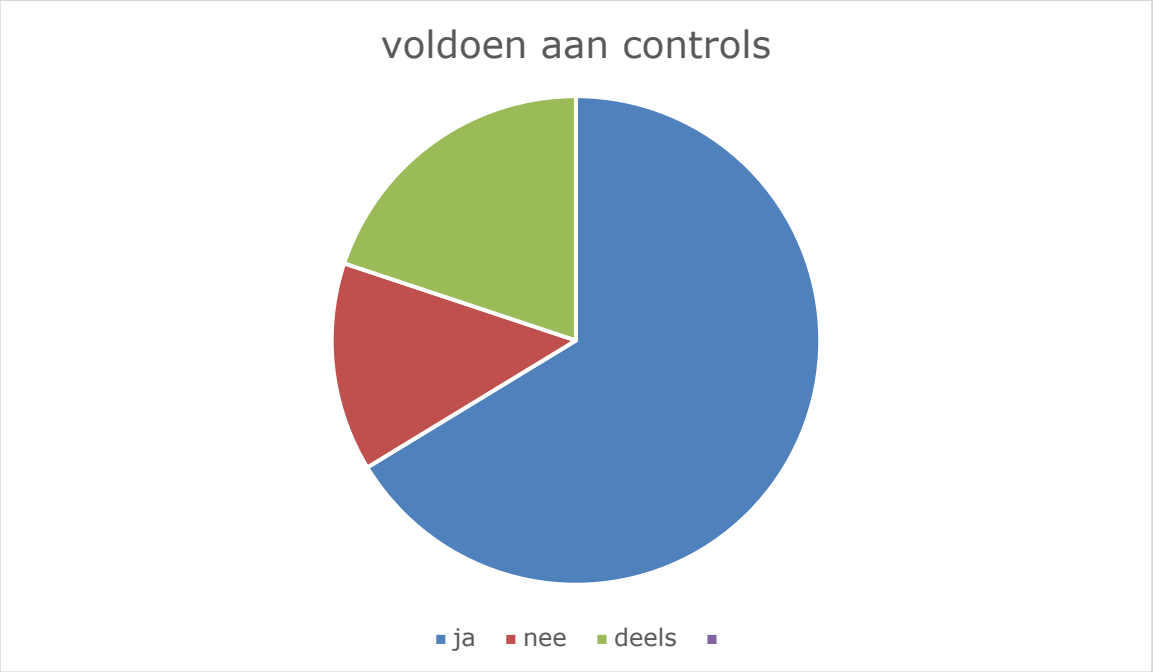
De VNG en IBD hebben samen begin 2021 een vernieuwd borgingsdocument opgesteld, met quickscans en controlevragen. De quickscans kunnen worden gebruikt om snel te meten waar de organisatie staat op de diverse thema's. Vervolgens kan een verdiepingsslag worden gemaakt met de control-vragenlijsten, opgesplitst in O-controls en P-controls (P-controls per afdeling). O ziet op organisatiemaatregelen (circa 221 controlevragen/normen) en P ziet op procesmaatregelen (circa 224 controlevragen/normen per afdeling/vakgebied). In de control-vragen wordt gevraagd om het volgende aan te geven:
(1) de mate waarin de maatregelen zijn geïmplementeerd;
(2) het volwassenheidsniveau per control (5 niveaus per set controlevragen/normen);
(3) de motivatie waarom voldaan is aan de omschrijving van het volwassenheidsniveau (en maatregel).

De vragen zijn opgesplitst in 7 onderdelen: beleid, processen, organisatorische inbedding, rechten van betrokkenen, samenwerking, beveiliging en verantwoording.

Tabel. In onderstaande tabel is de score per onderdeel uit de algemene controls (zowel o als p) weergegeven:

Score per onderdeel	**Ja**	**Nee**	**Gedeeltelijk**
Beleid	10	0	4
Processen	34	7	11
Organisatorische Inbedding	18	2	5
Rechten van betrokkenen	20	7	6
Samenwerking	8	1	0
Beveiliging	18	8	9
Verantwoording	12	0	1
Totaal	**120**	**25**	**36**

Grafiek. Dit levert de volgende cirkeldiagram op van de totaalscore.



Hieruit is af te leiden dat de Gemeente Barneveld goed in zicht heeft op wat wel, niet of deels geregeld is en waar nog aandacht aan besteed moet worden. Bij zaken die de score gedeeltelijk hebben gekregen, is de betreffende zaak veelal wel goed ingeregeld, maar ontbreekt een vastlegging van ongeschreven gedragsregels of is er bijvoorbeeld niet bij iedere applicatie een logging ingeregeld of zijn zaken niet automatisch maar alleen handmatig te wijzigen. Hierdoor wordt dan niet geheel aan de norm voldaan of is het volwassenheidsniveau minder hoog.

Verder worden een aantal zaken die op gedeeltelijk staan in de actualisering van beleid en de opstelling van nieuw beleid meegenomen. Overigens kan opgemerkt worden dat een 100% score nooit te garanderen is, omdat privacy & security vakgebieden zijn die continue in beweging zijn.

4. WERKZAAMHEDEN EN BEVINDINGEN

4.1 Privacybeleid

Op 1 april 2018 is het Privacybeleid in werking getreden. Op 30 mei 2018 is de gemeenteraad hierover geïnformeerd. Dit beleid implementeert de uitgangspunten en verplichtingen uit de AVG. De uitgangspunten rechtmatigheid, behoorlijkheid, transparantie, doelbinding, subsidiariteit, proportionaliteit, dataminimalisatie en vertrouwelijkheid worden omgezet in alle werkprocessen waarbinnen persoonsgegevens worden verwerkt. Er is beleid gevormd op hoe om te gaan met de rechten van betrokkenen, meldplicht datalekken, de functies van FG, PO en CISO en de gegegevensuitwisseling tussen verschillende domeinen en afdelingen.

Het nieuwe privacybeleid in op 11 mei 2021 vastgesteld door het college en is op 1 juni 2021 in werking getreden. De raad is hierover geïnformeerd en ook op de website is hier aandacht aan besteed. In zomer 2021 is er een begin gemaakt met de evaluatie van het cameratoezicht, waarbij de noodzakelijkheid van het cameratoezicht in de openbare ruimte wordt onderzocht en waarbij het cameratoezicht wordt getoetst aan de AVG. Deze evaluatie loopt door in 2022. Nadat de resultaten bekend zijn en indien het cameratoezicht voortgezet wordt, zal camerabeleid opgesteld worden.

4.2. Thuiswerken

In de periode (v.a. 14 maart 2020 tot einde verslagperiode 31 december 2021, maar duurt nog voort in 2022) dat er landelijk maatregelen afgekondigd zijn ter bestrijding van het Corona-virus heeft de Gemeente Barneveld lokaal ook maatregelen getroffen. Een daarvan is het thuiswerken voor alle medewerkers, tenzij dat niet mogelijk is vanwege de aard van de werkzaamheden (zoals (deel) publiekszaken, afvalophaaldienst, groenvoorziening e.d.).

Er is benadrukt dat de regels van privacy en informatiebeveiliging in acht genomen moeten worden. Deze zijn ook meermaals herhaald. Vanuit privacy is aangegeven dat het ongewenst en ook strijdig met het privacybeleid is dat medewerkers fysieke documenten meenemen met daarop persoonsgegevens of andere vertrouwelijke gegevens. Via de beveiligde netwerkomgeving zijn alle documenten beschikbaar.

Vanuit informatieveiligheid/-beveiliging zijn de regels voor thuiswerken nogmaals onder de aandacht gebracht. De handleidingen en uitleg staan op intranet. Daarbij zijn medewerkers erop geattendeerd dat ze met vertrouwelijke gegevens en informatie werken en er dus voor moeten waken dat huisgenoten daar geen kennis van kunnen nemen. Dat geldt ook voor het voeren van zakelijke gesprekken en online vergaderingen.

4.3. Register van verwerkingen

In 2021 is het register geactualiseerd. In zomer 2021 is de website volledig doorlopen op actualiteit en volledigheid, zodat geborgd is dat de juiste informatie verstrekt wordt.

In 2020 heeft de VNG de "Selectielijst 2020" vastgesteld en deze vervangt de Selectielijst 2017 (deze blijft nog wel van toepassing op archiefbescheiden van tussen 1-1-2017 en 31-12-2019). Gemeenten hanteren verplicht de bewaartermijnen in de Selectielijst. De actualisatie was nodig in verband met wijzigingen in wet- en regelgeving (zoals de AVG), het toevoegen van nieuwe bewaartermijnen voor o.a. algoritmes en redactionele verbeteringen. In 2021 zijn in het register van verwerkingen alle bewaartermijnen nagelopen en waar nodig zijn wijzigingen doorgevoerd, zodat het register voldoet aan de Selectielijst 2020.

4.4. Meldingen datalekken

IBD: Het jaar in cijfers

De IBD ontving het afgelopen jaar 2.487 aanvragen- en meldingen over informatiebeveiliging en 542 privacyaanvragen. De IBD registreerde 276 incidenten met een hulp-, coördinatie- of ondersteuningsvraag van gemeenten en ontving hierover ruim 1600 inkomende telefoongesprekken.

De IBD-CERT verstuurde 1.846 kwetsbaarheidsmeldingen waarvan 90 met een hoge kans op misbruik en een grote potentiële schade. De SMS-waarschuwing werd in 2021 vijf keer ingezet, waarvan twee keer voor de Log4J-problematiek.

De IBD organiseerde 82 onlinebijeenkomsten, zoals werkgroepen, intervisiebijeenkomsten, webinars en (be)spreekuren. De IBD streeft ernaar vooral onderlinge interactie tussen de deelnemers te stimuleren.

De website van de informatiebeveiligingsdienst werd ruim 135.000 keer bezocht. Op de website verschenen 27 nieuwe en bijgewerkte kennisproducten. De top 3 meest gedownloade producten waren dit jaar de BIO, de baselinetoets en de standaard verwerkersovereenkomst. De IBD voert het beheer over het VNG-privacyforum, dat inmiddels meer dan 4.700 gemeentelijke deelnemers heeft.

Cijfers Barneveld

In totaal zijn er in 2021 26 beveiligingsincidenten gemeld bij de Gemeente Barneveld. Nader onderzoek door de FG/PO/CISO wijst uit dat er geen beveiligingsincidenten gemeld moesten worden aan de AP. De AP registreert alle meldingen die door gemeenten gedaan worden. De AP reageert alleen in gevallen dat zij 'nader onderzoek' willen doen naar een door de gemeente gedane melding. In 2021 is daarvan geen sprake geweest. Ook heeft de AP geen waarschuwing gedaan of een dwangsom opgelegd aan de Gemeente Barneveld.

Nu er geen datalekken aan AP zijn gemeld, zijn er ook geen meldingen aan betrokkenen gedaan. Uit een analyse van de datalekken is gebleken dat het van belang is om blijvend aandacht te besteden aan bewustwording over omgang met bedrijfsmiddelen en/of verwerken van persoonsgegevens. Waar nodig zijn er technische maatregelen getroffen om de gebruikers te ondersteunen.

4.5. Rechten van betrokkenen

Er zijn in 2021 16 verzoeken binnengekomen. Van deze verzoeken zijn er 7 niet in behandeling genomen, omdat de verzoeken niet verder gespecificeerd zijn. Wat verder opvalt is dat 7 verzoeken zich richten op het Sociaal Domein en vooral als insteek hebben een soort van wantrouwen jegens gespreksvoerders en/ of ouders die onderling gebrouilleerd zijn. Er is in 2021 één klacht in verband met privacy ingediend, deze klacht is niet in behandeling genomen, omdat deze niet gespecificeerd was.

4.6. Bewaartermijnen

In het najaar van 2018 heeft team DIV de "Bezemdag" georganiseerd. Tijdens deze dag zijn veel papieren dossiers gearchiveerd of vernietigd. Ook is tijdens deze dag aandacht gevraagd voor het bewaren van persoonsgegevens in Outlook en op de harde schijf. Digitale dossiers en bijbehorende documenten en metadata worden door team DIV verwijderd na het verstrijken van de wettelijke bewaartermijnen. In overleg met team DIV is een start gemaakt met het project "Digitaal bezemen" om te zorgen dat op de harde schijven van medewerkers geen persoonsgegevens langer dan toegestaan bewaard blijven. Dit aandachtspunt wordt nadrukkelijk meegenomen in de Data Protection Impact Assessments (DPIA's). Er is overleg gevoerd over het opschonen van persoonsgegevens in de diverse applicaties. Bij nieuwe applicaties wordt de eis van automatisch verwijderen meegenomen.

In 2019 zijn digitale bezemdagen georganiseerd in verschillende teams en worden teams actief gewezen op het opschonen van mappen op netwerkschrijven en in e-mailboxen. Dit wordt in 2020 breder opgepakt. Door de coronapandemie is er door de meeste medewerkers bijna het hele jaar thuis gewerkt, waardoor het digitaal bezemen een lagere prioriteit heeft gekregen dan het goed beveiligd thuiswerken. Eind 2021 is het digitaal bezemen weer door enkele teams opgepakt en dit zal in 2022 breder uitgerold worden. Inmiddels is iedereen gewend geraakt aan het thuiswerken en weet men met welke privacy en informatiebeveiligings- aspecten rekening gehouden moet worden.

4.7. Verwerkers en verwerkersovereenkomsten

In 2018 en 2019 zijn de meeste verwerkersovereenkomsten afgesloten en in 2021 is met een aantal bestaande verwerkers en met een aantal nieuwe verwerkers een

(nieuwe) verwerkersovereenkomst afgesloten. Een actueel overzicht hiervan is beschikbaar. Bestaande verwerkers hebben niet gerapporteerd over incidenten.

In 2021 is bij hoofdovereenkomsten die werden gewijzigd dan wel verlengd ook meteen de door VNG/ IBD verplicht gestelde verwerkersovereenkomst afgesloten, zodat eerder afgesloten verwerkersovereenkomsten langzaam aan worden vervangen. Hierbij loopt de Gemeente Barneveld als verwerkingsverantwoordelijke geen risico, omdat eerder afgesloten verwerkersovereenkomsten vaak uitgebreider zijn dan de huidige verplicht gestelde verwerkersovereenkomst. Verder weten collega's ook de Privacy Officer te vinden als ze twijfelen of een verwerkersovereenkomst moet worden afgesloten en wordt een af te sluiten verwerkersovereenkomst ook altijd voorgelegd aan de Privacy Officer.

Er is in 2021 in een aantal gevallen afgeweken van de standaard en door VNG/IBD verplicht gestelde verwerkersovereenkomst. Dat is gedaan bij de volgende verwerkersovereenkomsten:

- Arbode Consultancy BV met betrekking tot de uitvoering van de offerte RI&E, ingangsdatum 1 april 2021;
- DTV Consultants met betrekking tot de uitvoering van een verkeersveiligheidsonderzoek;
- iBabs met betrekking tot een vergadersysteem t.b.v. bestuurlijke besluitvorming.

In al deze overeenkomsten is artikel 7 anders dan standaard geformuleerd. Artikel 7 verwijst voor het opschonen van gegevens na afloop van de hoofdovereenkomst naar de hoofdovereenkomst. In de genoemde overeenkomsten was het opschonen van gegevens echter niet geregeld in de hoofdovereenkomst.

4.8. Privacy in het Sociaal Domein

Tussen de afdeling Sociaal Domein, voornamelijk de juristen, de beleidsmedewerkers en de informatieadviseur, en de Privacy Officer is een goede samenwerking ontstaan. Indien nodig wordt tijdig de Privacy Officer geraadpleegd en om advies gevraagd.

Met ketenpartners waarmee de gemeente Barneveld samenwerkt of opdrachtgever voor is binnen het Sociaal Domein, wordt per proces beoordeeld of er een overeenkomst moet worden afgesloten en zo ja, wat voor een overeenkomst. Dit kan een verwerkersovereenkomst, een convenant of een andere vorm van een overeenkomst zijn om de privacy te waarborgen. Hierbij wordt nauw en in goed overleg samengewerkt met de afdeling Sociaal Domein.

De FG van Regio Foodvalley heeft in juni 2021 een signaal uitgestuurd dat de verwerkingen van data-analyse jeugdhulp en data-analyse leerplicht door het Knooppunt niet goed verwerkt worden. Hierop hebben de deelnemende gemeenten

gezamenlijk de verwerking stopgezet. Er is een DPIA uitgevoerd, waarin een aantal risico's naar voren zijn gekomen. Er zijn maatregelen vastgesteld om deze risico's te beperken, waaronder het opstellen van nieuwe/verbeterde werkprocesbeschrijvingen en het opnemen van de verwerking in het register van verwerkingen. Daarnaast zal begin 2022, een verwerkersovereenkomst worden opgesteld en worden de samenwerkingsovereenkomst en het convenant aangepast. Na het nemen van deze maatregelen zijn de verwerkingen die het Knooppunt doet in overeenstemming met de AVG en de informatieveiligheid-vereisten. Begin 2022 kan de verwerking naar verwachting weer opgestart worden.

4.9. Informatieveiligheid

De CISO is druk bezig geweest met het opleveren van de verantwoordingen in het kader van BAG, BGT, DigiD, Suwinet, BIG, ENSIA, BRP en PNIK. Daarnaast zijn er tal van maatregelen geëvalueerd (en eventueel bijgestuurd). De CISO acteert op alle lagen van de Gemeente Barneveld (Strategisch, Tactisch en Operationeel). De CISO stelt zowel beleidsstukken op als dat de CISO langs verschillende teams gaat voor bewustwordingstrainingen. Op dit moment voldoet de Gemeente Barneveld aan alle wettelijke verplichtingen rondom informatiebeveiliging.

4.10. Data Protection Impact Assessments

In 2018 en 2019 zijn in totaal 23 Data Protection Impact Assessments (DPIA's) uitgevoerd. In 2020 zijn er 2 DPIA's uitgevoerd en in 2021 is er één DPIA uitgevoerd en zijn er 2 DPIA's uit 2020 verder uitgewerkt.

In 2022 zullen er 18 DPIA's voor de onderstaande vakgebieden worden uitgevoerd, waarbij dit voor de meeste vakgebieden een herziening van de DPIA uit 2018/2019 betreft:

Veiligheid	RIEC IS
	Damocles
Personeelszaken	AFAS (personeelsdossier)
Woonurgentie	Woonurgentieverklaring
Belastingen	Heffingen- en invorderingsadministratie
	Kwijtschelding gemeentelijke belastingen
	Innen vorderingen privaat en publiekrecht
Schuldhulpverlening	Vroegsignalering schuldhulp voorafgaand
	Schuldhulpverlening
Handhaving	Bodycams BOA's (Handhaving)
	BRS (Handhaving)
Beveiligingscamera's	Beveiligingscamera's stations toiletten en fietsenstallingen
Horeca-aanvragen	Horeca aanvraag

Wmo	WMO - materiele hulp
	WMO - niet-materiele hulp
Participatiewet	IOAW- en IOAZ-uitkering
	Participatiewet (uitkering levensonderhoud, bijzondere bijstand, minimaregelingen)
	Participatiewet (reintegratie)

In 2023 zullen er 4 DPIA's voor de onderstaande vakgebieden worden uitgevoerd, waarbij dit voor de meeste vakgebieden een herziening van de DPIA uit 2019/2020 betreft:

Onderwijs	Onderwijs - Leerlingenvervoer (melding en aanvraag)
	Onderwijs - Uitvoering Leerplichtwet en RMC- wet
Jeugdzorg	Jeugdzorg
	MDO-lokaal

In 2021 uitgevoerde DPIA's:

- Nieuwe Zaaksysteem
- Suite4Sociaal Domein Regie (vervolg op 2020)
- Camera's gemeentehuis
- Vroegsignalering schuldhulp voorafgaand (vervolg op 2020)

De DPIA's vonden plaats aan de hand van een vragenlijst. Deze vragenlijst is deels gebaseerd op de vragenlijst van de beroepsvereniging voor IT-auditors NOREA en door de privacy officer aangepast en verder aangevuld. Hierin wordt gevraagd naar de verwerkingsverantwoordelijke en verwerkers(overeenkomsten), nieuwe technieken, noodzaak van gegevensverwerking, aard van de persoonsgegevens (bijzonder of gevoelig), gegevensuitwisseling intern en extern, doelbinding, grondslag, transparantie, actualiteit, integriteit en beschikbaarheid van persoonsgegevens, rechten van betrokkenen, bewaartermijnen en beveiliging.

Per team wordt een rapportage opgesteld met bevindingen, conclusies en aanbevelingen. Wanneer een werkproces op korte termijn gewijzigd wordt of als sprake is van een pilot, wordt een aparte rapportage opgesteld.

In de gehouden DPIA's komen de volgende risico's naar voren:

1. De aanwezigheid van een schaduwarchief. Als de gegevens (gegevens en alle documenten) te lang worden bewaard, houdt dit in dat er een risico is op onrechtmatig gebruik (voor andere doelen) of verlies van gegevens.
2. Er worden gegevens onbeveiligd verzonden per e-mail.
3. Er worden gevoelige gegevens bewaard in een algemeen toegankelijke map op een netwerkschijf.
4. Er wordt via Whatsapp gecommuniceerd met burgers.

De volgende maatregelen zijn reeds genomen:

1. Diverse teams hebben hun (schaduw)archieven en mappen (fysiek en digitaal) opgeschoond en belangrijke stukken laten archiveren.
2. Er wordt steeds meer beveiligd gemaild met een wachtwoord.
3. Er wordt niet meer gecommuniceerd met burgers via Whatsapp app, hooguit voor een afspraakbevestiging of iets anders algemeens, maar niet meer dossier inhoudelijk. Daarvoor wordt gebruik gemaakt van e-mail of van de berichtenservice Signal die beter beveiligd is dan Whatsapp app.

Er zijn afspraken gemaakt over de termijn waarop andere maatregelen worden genomen.

4.11. Bewustwording

Meer bewustwording van privacyrisico's onder medewerkers is in 2021 op voornamelijk door middel van berichten op intranet gestalte gegeven.

Vanaf medio maart is het door de coronapandemie en het thuiswerken niet meer mogelijk geweest voor FG en PO om regelmatig rondjes door de gangen te lopen en kaartjes neer te zetten als iemand zijn beeldscherm niet heeft vergrendeld of zijn pasje heeft laten liggen… in 2022 zal dat weer opgepakt worden, zodra er weer meer op kantoor gewerkt mag worden.

Net als in voorgaande jaren, zijn er in 2021 workshops over Privacy en Informatiebeveiliging gehouden. Deze workshop is verplicht voor alle nieuwe medewerkers. Vanaf najaar 2020 zijn deze workshops online gehouden.

Belangrijk voor de bewustwording is ook de bekendheid en benaderbaarheid van de PO om als vraagbaak te fungeren. Hiervan is veel gebruik gemaakt.

4.12. Overige zaken

Ook in 2022 zijn er wetswijzigingen te verwachten, waarin gegevensverwerking voorkomt.

Zo treedt op 1 mei 2022 de Wet open Overheid (Woo) als opvolger van de Wet openbaarheid van bestuur (Wob) in werking. Het uitgangspunt van de Woo is een actievere openbaarmakingsverplichting en een ruimere openbaarmaking in geval van passieve openbaarmaking (als een verzoek is ingediend). Ook wordt gestreefd naar het zoveel mogelijk digitaal communiceren met de indieners van verzoeken. Naast nieuwe mogelijkheden, levert dit vanuit privacy & security ook risico's op, zodat bij implementatie betrokkenheid PO, CISO en FG van belang is.

En vermoedelijk treedt Wet Aanpak Meervoudige problematiek Sociaal Domein (WAMS) eind 2022 in werking. In de WAMS wordt wettelijke borging van de regionale meldpunten voorbereid. Dit wetsvoorstel, voortvloeiend uit het traject Uitwisseling

Persoonsgegevens (UPP) is in 2021 in consultatie geweest. De wet WAMS betreft een aanpassing van de Wmo en regelt een basis voor gegevensdeling in het sociaal domein en een gemeentelijk meldpunt niet-acuut. Ook deze wet levert, naast nieuwe mogelijkheden, vanuit privacy & security risico's op, zodat bij implementatie betrokkenheid PO, CISO en FG van belang is.

In 2022 zal ook de eerste verplichte externe audit inzak de Wet politiegegevens (Wpg) plaats moeten vinden. Deze wet heeft raakvlakken met de AVG en stelt vergelijkbare eisen aan de verwerking van gegevens. Wat betreft de taken van de FG is dit een uitbreiding en komen er een aantal taken bij die specifiek gelden voor de Wpg. Hierover worden in 2022 afspraken over taken, rollen en bevoegdheden gemaakt met de handhavers/BOA's van de gemeente.

5. AANBEVELINGEN EN ACTIES

5.1. Aanbevelingen

Belang: het is belangrijk om het bewustzijn over het belang van het zorgvuldig omgaan met en verwerken van persoonsgegevens blijvend onder de aandacht te houden bij de medewerkers. Daarbij is de combinatie privacy en informatieveiligheid een vast gegeven.

Aanbeveling: voor een blijvend bewustzijn regelmatig berichten op intranet plaatsen. Ook kan met de teamleiders afgesproken worden dat de Privacy Officer met enige regelmaat of incidenteel aanschuift bij teamoverleggen om in algemene zin of aan de hand van een specifieke casus het bewustzijn over het omgaan met persoonsgegevens hoog te houden. Dat is in 2019 meerdere keren gedaan, maar was in 2020 vanaf medio maart niet meer mogelijk vanwege de coronapandemie en het vele thuiswerken. Dit is vervolgens online opgepakt en zal in 2022 online of zodra het weer mogelijk is fysiek voortgezet worden.

Vanuit informatieveiligheid blijft aandacht gevraagd worden voor het vergrendelen van het beeldscherm als de werkplek verlaten wordt. Belangrijk is het toegangspasje dan ook mee te nemen. Hiermee wordt voorkomen dat anderen zich eenvoudig toegang verschaffen tot vertrouwelijke gegevens, persoonsgegevens en bedrijfsgevoelige documenten en gegevens. Verder is het van belang dat fysieke documenten veilig achter slot en grendel liggen en dat bezoekers tot aan de deur worden begeleid. Ook bij het thuiswerken moet worden gelet op het opbergen van documenten, omdat het niet de bedoeling is dat onbevoegden, denk aan huisgenoten, kennis kunnen nemen van vertrouwelijke informatie.

Belang: het is belangrijk om de bescherming van persoonsgegevens goed te borgen. Zowel vanuit privacyoverwegingen als gezien vanuit de beveiliging van informatie en het (be)veilig(d) omgaan met informatie, gegevens en documenten is dit van groot belang.

Aanbeveling: in 2020 is uitgezocht welke protocollen en procedures er op afdelingsniveau beschikbaar en/of gewenst zijn. In 2021 is daar een begin mee gemaakt en in 2022 zal verder opgepakt worden en waar nodig zullen deze protocollen en procedures opgesteld gaan worden. Als deze zaken geregeld zijn, is de bescherming van persoonsgegevens beter geborgd. Het inzetten van een mystery guest is een mogelijkheid om te beoordelen hoe het niveau van borging is.

5.2. Acties voor 2022

In de voorgaande hoofdstukken is aangegeven welke werkzaamheden in 2021 zijn uitgevoerd en in paragraaf 5.1. worden de aanbevelingen genoemd. In deze laatste paragraaf wordt nader ingegaan op de acties die hiervoor al kort genoemd zijn. In 2022 worden de onderstaande acties opgepakt, waarover in het Jaarverslag FG 2022 gerapporteerd zal worden.

- DPIA's: evalueren van de opgepakte en uitgevoerde van de uit de rapportages voortgekomen aanbevelingen en maatregelen. Daarna toezien op de naleving ervan.
- DPIA's: herzien en actualiseren van de in 2018/2019 uitgevoerde DPIA's (3-jaarlijkse herziening);
- Continue aandacht houden voor het belang van het afsluiten van verwerkersovereenkomsten en het overzicht actueel houden. Verouderde overeenkomsten actualiseren en nieuwe overeenkomsten afsluiten met nieuwe verwerkers.
- Vervolg workshops Privacy & Informatieveiligheid voor nieuwe medewerkers.
- Op verzoek aansluiten bij teamoverleggen of afdelingsoverleggen om privacy binnen een bepaald vakgebied te bespreken.
- Vervolg opschoonacties, waarbij de wettelijke bewaartermijnen goed in acht genomen moeten worden. Bij het opschonen van documenten en (persoons)gegevens, inclusief metadata, moet niet vergeten worden dat veel medewerkers schaduwbestanden hebben in ordners en op netwerkschijven. Ook de gegevens en documenten in e-mailberichten mogen daarbij niet vergeten worden. De in 2019 ingezette actie om ook digitaal te bezemen krijgt in 2022 een vervolg.
- In 2020 is uitgezocht welke actuele protocollen en procedures er gemeentebreed of op afdelingsniveau zijn of wenselijk zijn. Met het opstellen of actualiseren van protocollen en procedures over de wijze van omgang met persoonsgegevens is in 2021 een begin gemaakt, zodat deze in 2022 opgesteld kunnen gaan worden.
- Actiepunten zelfevaluatie/borging oppakken.
- Actualiseren camerabeleid.

gemeente
Barneveld

Raadsmemo Jaarverslag Functionaris Gegevensbescherming 2021

Datum: 3 februari 2022

Onderwerp: Jaarverslag FG 2021

Ter attentie van: De raad

Afzender: College van Burgemeester en Wethouders

Portefeuillehouder: A.H. van de Burgwal

Mail behandelaar s.beekman@barneveld.nl *Telefoonnummer* 381

Samenvatting
Op 25 mei 2018 is de Europese Algemene verordening gegevensbescherming (AVG) van toepassing geworden in de hele Europese Unie. In Nederland is op die dag de Wet bescherming Persoonsgegevens komen te vervallen. Het jaarverslag Functionaris Gegevensbescherming 2021 geeft weer wat de Gemeente Barneveld in 2021 heeft ondernomen om aan de vereisten van de AVG te voldoen.

Doel
Het doel van de memo is om de raad te informeren over het jaarverslag. De AVG en het Privacybeleid van de Gemeente Barneveld schrijven voor dat de FG jaarlijks voor 1 maart verslag uitbrengt aan de bestuursorganen. Het onderhavige verslag wordt dan ook uitgebracht aan het college van burgemeester en wethouders, de burgemeester en de gemeenteraad van Barneveld.

Inhoud memo
In 2021 zijn de volgende zaken gerealiseerd:
- het Privacybeleid is geactualiseerd en vastgesteld;
- het register van verwerkingen is geactualiseerd;
- er zijn nieuwe of geactualiseerde verwerkersovereenkomsten afgesloten met vele verwerkers;
- er zijn intern veel adviezen gegeven en (online) workshops gehouden over privacy en informatieveiligheid;
- er zijn meerdere Data Protection Impact Assessments (DPIA) uitgevoerd, waarmee een goede risico-analyse gemaakt kan worden over hoe er per vakgebied omgegaan wordt met het verwerken van (persoons)gegevens. In 2021 is een deel van de 2018/2019 uitgevoerde DPIA's herzien, omdat de AVG vereist dat DPIA's iedere 3 jaar uitgevoerd worden. In 2022 wordt hiermee verder gegaan.

Vanwege de coronapandemie is er vanaf medio maart 2020 en in heel 2021 door de meeste medewerkers veel vanuit huis gewerkt. Thuiswerken brengt risico's met zich mee op het gebied van privacy en informatiebeveiliging, zodat daar extra aandacht voor gevraagd is in meerdere nieuwsbrieven en berichten op intranet.

Vervolg
Met het publiceren van het Jaarverslag FG 2021 op de website van de gemeente voldoet het college aan de in de AVG en het Privacybeleid opgenomen informatieverplichting. Hiermee geeft het college aan uw raad en aan de inwoners en andere belangstellenden opening van zaken over wat de Gemeente Barneveld in 2021 heeft ondernomen om aan de vereisten van de AVG te voldoen. In het verslagjaar wordt toegelicht welke werkzaamheden zijn uitgevoerd en wat de acties voor het komende jaar zijn.