gemeente
Barneveld

Raadsmemo Jaarverslag Functionaris Gegevensbescherming 2020

Datum: 28 januari 2021

Onderwerp: Jaarverslag FG 2020

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 2020 geeft weer wat de Gemeente Barneveld in 2020 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 2020 zijn de volgende zaken gerealiseerd:
- het register van verwerkingen is geactualiseerd en aangevuld met verwerkingen waarin de gemeente verwerker is in plaats van verwerkingsverantwoordelijke zoals in bijna alle gevallen;
- er zijn nieuwe of geactualiseerde verwerkersovereenkomsten afgesloten met vele verwerkers;
- er zijn intern veel adviezen gegeven en workshops gehouden over privacy en informatieveiligheid;
- in 2018 en 2019 is voor veel vakgebieden een 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 2020 zijn er weer een aantal DPIA's uitgevoerd en de laatste paar PIA's volgen in 2021. Ook worden in 2021 de in 2018 uitgevoerde DPIA's herzien, omdat de AVG vereist dat DPIA's iedere 3 jaar uitgevoerd worden.

Vanwege de coronapandemie is er vanaf medio maart 2020 door de meeste medewerkers alleen 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 2020 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 2020 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.

gemeente Barneveld

Jaarverslag

Functionaris Gegevensbescherming 2020

Jaarverslag

Functionaris Gegevensbescherming 2020

Opdrachtgever:	gemeente Barneveld Afdeling Bestuur & Dienstverlening
Auteur:	Sascha Beekman, Functionaris Gegevensbescherming
Datum:	28 januari 2021

Inhoud

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 2020 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 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 alleen 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.

De laatste Data Protection Impact Assessments (DPIA's), waarmee een goede risico-analyse gemaakt kan worden over hoe er per vakgebied omgegaan wordt met het verwerken van (persoons)gegevens, zijn in 2020 afgerond. De rapportages daarover met bevindingen, conclusies en aanbevelingen zijn afgerond en de daarin opgenomen aanbevelingen en – waar nodig – te nemen maatregelen zijn besproken met de teamleiders en binnen de teams opgepakt. Eind 2020 en begin 2021 zal gebruikt worden om de aanbevelingen en te nemen maatregelen te evalueren en te beoordelen hoe deze zijn opgepakt en uitgevoerd.

Op Valentijnsdag zijn chocolaatjes uitgedeeld met daarop het gemeentelogo en de tekst 'love privacy' om de medewerkers te bedanken voor het privacy-bewustzijn.
Er dient 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 2020 stond al 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.

In 2021 is niet alleen de borging van belang, maar zal ook extra aandacht besteed worden 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. In 2021 zal tevens het privacybeleid herzien worden en zal een camerabeleid opgesteld worden, omdat er steeds meer gebruik gemaakt wordt van cameratoezicht, waarbij de mogelijkheden en risico's voor privacy en informatiebeveiliging goed tegen elkaar afgewogen moeten worden.

2. WETTELIJK KADER

- **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.

- **Specifieke wetgevende ontwikkelingen, jurisprudentie en nieuwsberichten van Autoriteit Persoonsgegevens**

1. AP nieuwsbericht 24 april 2020

De European Data Protection Board (EDPB) heeft twee nieuwe guidelines vastgesteld gerelateerd aan de bestrijding van het coronavirus. Het gaat om guidelines voor het verwerken van gezondheidsgegevens voor wetenschappelijk onderzoek en om guidelines rondom het gebruik van locatiegegevens en rondom het gebruik van apps die inzage geven in contacten tussen mensen, de zogenoemde (contact) tracing apps. De guidelines zijn onder meer bedoeld voor Europese overheden, bedrijven en organisaties zoals ziekenhuizen.

2. AP nieuwsbericht 17 juni 2020

EDPB: Grenzen EU weer open tijdens corona? Let op privacy!
Steeds meer grenzen tussen EU-lidstaten gaan weer open, nu de coronamaatregelen versoepeld zijn. De lidstaten kunnen hierbij extra maatregelen willen nemen. Bijvoorbeeld coronatests aan de grens, een verplichte medische verklaring of verplicht

gebruik van een corona-app. De Europese privacytoezichthouders waarschuwen dat de EU-lidstaten hierbij het recht op privacy moeten blijven beschermen. En dat samenwerking tussen corona-apps in verschillende landen niet mag leiden tot schending van de privacywetgeving. Dat stellen de EU-privacytoezichthouders in 2 verklaringen die ze aannamen tijdens een vergadering van de European Data Protection Board (EDPB) op 16 juni 2020.

Maatregelen grenzen: In de verklaring over maatregelen bij grenzen benadrukt de EDPB dat de privacywetgeving van kracht blijft, ook in deze tijd. Natuurlijk moet corona bestreden worden. Maar daarbij moeten fundamentele rechten en vrijheden beschermd blijven, aldus de EDPB.

Samenwerking tussen apps: Verschillende landen in de EU gebruiken 'corona contact tracing apps'. Met het openen van de grenzen willen overheden dat de verschillende nationale apps kunnen samenwerken. De EDPB stelt in de verklaring over de samenwerking tussen corona-apps dat het delen van data tussen verschillende apps alleen kan met de vrijwillige deelname van de gebruiker. Daarbij stelt de EDPB dat die samenwerking tussen apps ('interoperabiliteit') niet mag leiden tot het verzamelen van meer data dan nodig. De EDPB benadrukt tot slot dat samenwerking tussen de apps kan leiden tot verhoogde risico's voor gegevensbescherming. Overheden moeten daar dus heel voorzichtig mee omgaan en alle mogelijke opties overwegen.

3. AP nieuwsbericht 23 juli 2020

AVG-guidelines over de PSD2-richtlijn open voor consultatie: De European Data Protection Board (EDPB) heeft guidelines opgesteld over de verhouding tussen de PSD2-richtlijn en de Algemene verordening gegevensbescherming (AVG). De openbare consultatie van deze guidelines loopt tot en met 16 september 2020.
PSD2: In 2019 is de nieuwe Europese richtlijn voor betaaldiensten in Nederland in werking getreden, Payment Service Directive 2 (PSD2). Deze richtlijn regelt onder meer dat niet alleen banken maar ook andere partijen toegang mogen hebben tot een betaalrekening. Dat mag onder bepaalde voorwaarden, zoals toestemming van de rekeninghouder. De bescherming van de privacy van consumenten is een belangrijk onderdeel van PSD2, omdat betaalgegevens gevoelige financiële persoonsgegevens zijn.
Guidelines PSD2 & AVG: Deze guidelines geven aanbieders van betaaldiensten meer duidelijkheid over de wijze waarop zij persoonsgegevens kunnen verwerken. De guidelines besteden onder meer aandacht aan toestemming, dataminimalisatie, beveiliging en transparantie.

4. AP nieuwsbericht 8 september 2020

Consultatie nieuwe guidelines EDPB: De European Data Protection Board (EDPB) heeft 2 nieuwe guidelines opgesteld: over de begrippen 'verantwoordelijke' en 'verwerker' en over targeting van gebruikers van sociale media. Beide (Engelstalige) guidelines staan nu open voor feedback.

Guidelines ‘verantwoordelijke’ en ‘verwerker’: Sinds de Algemene verordening gegevensbescherming (AVG) van toepassing is, zijn er veel vragen over de begrippen ‘verantwoordelijke’ en ‘verwerker’ en in hoeverre die zijn gewijzigd door de AVG. Vooral als het gaat om gezamenlijke verantwoordelijkheid en de verplichtingen voor verwerkers. Deze guidelines geven uitleg over de verschillende begrippen. Ook gaan de guidelines in op de belangrijkste gevolgen van deze begrippen voor verantwoordelijken, verwerkers en gezamenlijke verantwoordelijken.

Guidelines targeting sociale media: Targeting van gebruikers van sociale media is een manier om gericht te kunnen adverteren. Het is onderdeel van het verdienmodel van veel aanbieders van sociale media. Deze guidelines richten zich op de rollen en verantwoordelijkheden van adverteerders en aanbieders. De guidelines gaan daarbij onder meer in op de privacyrisico’s voor gebruikers van sociale media en op de belangrijkste vereisten uit de privacywetgeving, zoals de juridische basis voor de verwerking.

5. AP nieuwsbericht 11 november 2020

Aanbevelingen EDPB voor doorgifte persoonsgegevens na Schrems II-uitspraak (vervolg op: Statement on the Court of Justice of the European Union Judgment in Case C-311/18 - Data Protection Commissioner v Facebook Ireland and Maximillian Schrems d.d. 17 juli 2020)

De European Data Protection Board (EDPB) heeft aanbevelingen opgesteld voor de doorgifte van persoonsgegevens naar derde landen. Dat zijn landen waar persoonsgegevens minder goed beschermd zijn dan in de EU. De EDPB wil het bedrijfsleven hiermee meer duidelijkheid geven, nadat het Europese Hof van Justitie het EU-VS Privacy Shield ongeldig verklaarde. In juli concludeerde de hoogste Europese rechter in de Schrems II-uitspraak dat de bescherming van persoonsgegevens in de VS ernstig tekortschiet, ondanks het Privacy Shield. Dat waren de afspraken tussen de EU en de VS op basis waarvan bedrijven persoonsgegevens vanuit de EU mochten doorgeven aan de VS. Met de uitspraak zette het Hof een streep door het Privacy Shield. Alleen als organisaties kunnen waarborgen dat gegevens net zo goed beschermd worden als in de EU, mogen zij nog persoonsgegevens doorgeven aan de VS. En aan andere landen waarmee de EU geen (geldige) afspraken heeft over bescherming van persoonsgegevens.

Modelcontracten: De meest praktische oplossing voor bedrijven die persoonsgegevens willen doorgeven naar derde landen, is het gebruik van modelcontracten (ook wel standaardbepalingen, standard contractual clauses of SCC’s genoemd). Maar dat mag in de meeste gevallen alléén als een bedrijf voldoende aanvullende maatregelen neemt om de veiligheid van de doorgifte te waarborgen.

Aanbevelingen EDPB: Om bedrijven te helpen die bescherming te waarborgen, heeft de EDPB aanbevelingen opgesteld voor aanvullende maatregelen bij het gebruik van

'doorgifte-instrumenten', waaronder modelcontracten. De EDPB noemt verschillende aanvullende maatregelen die bedrijven kunnen overwegen, zoals goede encryptie en pseudonimisering. Bedrijven zullen per geval moeten bekijken welke maatregel of combinatie van maatregelen nodig is om persoonsgegevens goed te beschermen. Zie verder:

- Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data
- Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.

Bij twijfel: houd data in EU
Het zal niet altijd mogelijk zijn om aanvullende maatregelen te treffen die persoonsgegevens voldoende beschermen. Sommige landen beschermen privacy en andere grondrechten onvoldoende. Daar hebben Europese bedrijven en Europese privacytoezichthouders weinig directe invloed op. Als bedrijven persoonsgegevens willen opslaan in landen waar persoonsgegevens minder goed worden beschermd, is het hun eigen verantwoordelijkheid om te waarborgen dat dit alsnog net zo veilig gebeurt. Is er na nader onderzoek nog steeds enige twijfel over de veiligheid van doorgifte van persoonsgegevens? Stop dan met de doorgifte of begin niet aan een nieuwe doorgifte. Houd data dan in de EU.

Inzage door veiligheidsdiensten VS: Veel bedrijven slaan data op in de VS. Nu heeft de Europese rechter dit land specifiek benoemd als land waar persoonsgegevens niet goed beschermd zijn. De veiligheidsdiensten in de VS mogen alle persoonsgegevens op servers in de VS inzien en gebruiken. Ook kunnen deze diensten persoonsgegevens al onderscheppen vóórdat ze in de VS aankomen. Het is daarom niet altijd mogelijk om te voorkomen dat de Amerikaanse veiligheidsdiensten inzage krijgen in persoonsgegevens die naar de VS worden doorgegeven. Bovendien is de rechtsbescherming door een onafhankelijke rechter onvoldoende geregeld in de VS, concludeerde het Europese Hof van Justitie. Het is dus van groot belang dat de VS zorgen voor een betere bescherming van persoonsgegevens. En het is nu aan de Amerikaanse regering en de Europese Commissie om te onderzoeken of er vervanging kan komen voor het Privacy Shield.

6. <u>AP nieuwsbericht 26 november 2020</u>

De European Data Protection Board (EDPB) heeft een verklaring gepubliceerd over de toekomstige e-Privacyverordening. In deze verklaring uit de EDPB zorgen over het toezicht op de e-Privacyverordening.

De EDPB, het samenwerkingsverband van privacytoezichthouders uit de Europese Unie (EU), heeft zich uitgesproken over het toezicht op de e-Privacyverordening. Deze verordening moet de e-Privacyrichtlijn uit 2002 gaan vervangen. De EDPB vindt dat het toezicht op verwerkingen van persoonsgegevens onder de e-Privacyverordening zou moeten worden toevertrouwd aan dezelfde nationale autoriteiten die toezicht houden op de Algemene verordening gegevensbescherming (AVG). Dat zorgt voor een hoog

niveau van bescherming, een gelijk speelveld en een geharmoniseerde interpretatie en handhaving door de EU, aldus de EDPB. Verder benadrukte de EDPB haar eerdere standpunt dat de e-Privacyverordening het beschermingsniveau van de huidige de e-privacyrichtlijn niet zou mogen verlagen. Ook zou de e-Privacyverordening de AVG moeten aanvullen, door sterke waarborgen te bieden voor vertrouwelijkheid en bescherming van alle types van elektronische communicatie.

- **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."*

<u>Trends en ontwikkelingen</u>
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

<u>Focusgebieden</u>
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.

<u>Risicogestuurd toezicht</u>
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 (interim) Privacy Officer (PO) en een Functionaris Gegevensbescherming (FG) aangewezen door het college. Deze onderlinge relaties en verantwoordingen blijken uit het door het college vastgestelde Privacybeleid dat op 1 april 2018 in werking is 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 2020:

In de periode vanaf oktober 2018 tot en met maart 2020 zijn de Data Protection Impact Assessments (DPIA's) uitgevoerd. De rapportages van deze DPIA's in het eerste kwartaal van 2020 afgerond. Het tweede en derde kwartaal van 2020 zijn gebruikt om de uit de DPIA's voortvloeiende acties op te pakken en uit te voeren.

Het Register van Verwerkingen is in het voorjaar van 2019 afgerond, waarna het register via de website is ontsloten door bij ieder product en bij iedere dienstverlening van de gemeente Barneveld een kopje "registratie en verwerking van uw gegevens" te vermelden. In 2020 is het register geactualiseerd en aangevuld met een gedeelte waarin de Gemeente Barneveld verwerkers is in plaats verwerkingsverantwoordelijke. Hierdoor zijn de verschillende verwerkingen nog beter en completer in beeld.

In de december 2020 is het borgingsdocument dat VNG en IBD hebben ontwikkeld, ingevuld, waarmee gelijk evaluatie is uitgevoerd op de beoordeling van het borgingsdocument van december 2019. Een deel van de daaruit in december 2019 voortgekomen acties zijn in 2020 opgepakt. De uit de nieuwe beoordeling en evaluatie voortkomende acties worden in 2021 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.

3.3 Verantwoording Privacy Officer

Overzicht uitgevoerde werkzaamheden in 2020:

PIA's uitvoeren	In 2020 zijn op risicovolle (interne) processen DPIA's uitgevoerd, met name processen binnen Domein Sociaal
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), het updaten van de Regeling gegevensverstrekking Basisregistratie personen en de beleidsregels briefadres opgesteld en vastgesteld.
Instellen + vullen register van verwerkingen	Nieuwe processen worden toegevoegd en wijzigingen in processen worden in het register doorgevoerd.
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 meerder 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	Sinds 1 februari 2019 wordt de PO- functie extern ingevuld voor 16 uur per week. Deze PO heeft uitvoering gegeven aan: - Toetsen / opstellen verwerkersovereenkomsten - Toetsen/ opstellen convenanten - Verbeteringsslag register van verwerkingen - Uitvoeren PIA's - Behandelen privacy vraagstukken - Signaleringsfunctie in organisatie - Sparringspartner voor de organisatie

	Eind 2020 is de vacature voor de PO- functie opnieuw uitgezet.

3.4 Verantwoording CISO

Overzicht uitgevoerde werkzaamheden in 2020:

Bewustwording privacy en informatiebeveiliging	- Samen met de PO zijn workshops voor medewerkers verzorgd. - Op verzoek zijn de CISO of PO bij teamoverleggen aanwezig geweest. - 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.

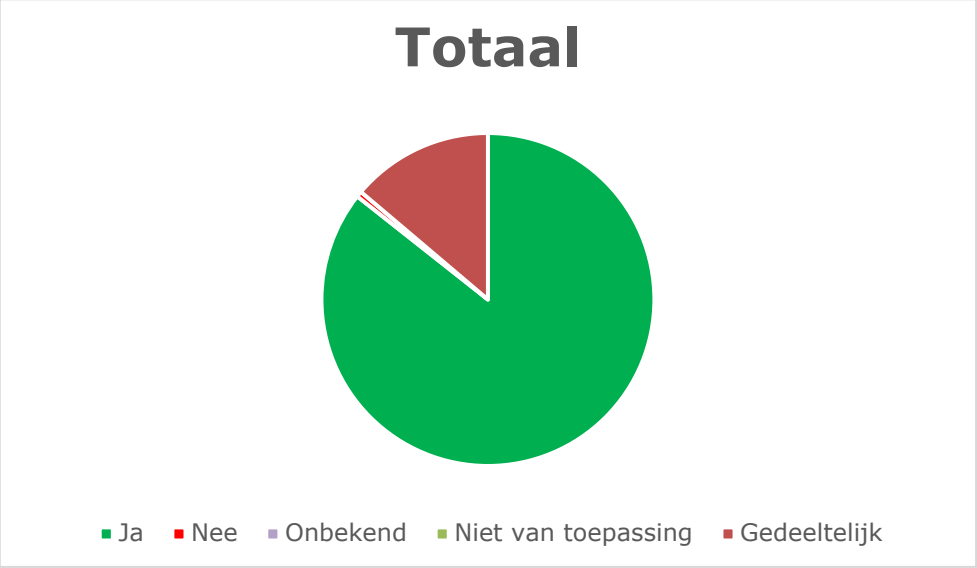
3.5 Borging

De VNG en IBD hebben samen een borgingsdocument opgesteld, waarin circa 190 vragen zijn opgenomen die zowel op de AVG betrekking hebben als op de maatregelen die de BIO (voorheen BIG) voorschrijft, onderverdeeld naar de aandachtsgebieden beleid, processen, organisatorische inbedding, rechten van betrokkenen, samenwerking, beveiliging en verantwoording.

In onderstaande tabel is de score per onderdeel weergegeven (stand van zaken december 2020):

Score per onderdeel	**Ja**	**Nee**	**Onbekend**	**N.v.t.**	**Gedeeltelijk**
Beleid	14	0	0	0	2
Processen	30	0	0	0	4
Organisatorische Inbedding	33	0	0	0	9
Rechten van betrokkenen	26	0	0	0	3
Samenwerking	18	0	0	0	1
Beveiliging	17	1	0	0	3
Verantwoording	17	0	0	0	3
Totaal	**155**	**1**	**0**	**0**	**25**

Dit levert de volgende cirkeldiagram op van de totaalscore.



Hieruit is af te leiden dat de Gemeente Barneveld steeds beter in beeld heeft 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 (werk)procesbeschrijving. De zaken die in 2019 een 'nee'-score kregen, zijn in 2020 opgepakt, waardoor deze op een na allemaal op 'ja' of 'gedeeltelijk' zijn komen te staan. Hieruit is af te leiden dat er 2020 een flinke verbeteringsslag is doorgevoerd. Overigens is bij de zaken met scores 'nee' of 'gedeeltelijk' weinig risico aanwezig, aangezien het hier voornamelijk borging betreft.

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.

In het najaar van 2019 en in het najaar van 2020 is het beleid geëvalueerd en eind 2020 is het beleid geactualiseerd en herzien, zodat het nieuwe privacybeleid in het eerste kwartaal van 2021 vastgesteld kan worden. Behalve het privacybeleid is er ook een camerabeleid opgesteld, omdat er steeds meer gebruik gemaakt wordt van cameratoezicht. Dit beleid zal eveneens in het eerste kwartaal van 2021 worden vastgesteld.

4.2. Thuiswerken

In de periode (v.a. 14 maart 2020 tot…?) 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

Alle werkprocessen zijn gedurende 2018 geanalyseerd op de verwerking van persoonsgegevens en in overleg met bijna alle teams is het register van verwerkingen opgesteld. De ontbrekende processen zijn in het eerste halfjaar van 2019 aangevuld.

Vervolgens is de informatie uit het register op de website ontsloten voor een ieder die daarin geïnteresseerd is.
Bij ieder product en bij iedere dienstverlening van de Gemeente Barneveld is op de gemeentelijke website een kopje geplaatst met "registratie en verwerking van uw gegevens".

In 2020 is het register geactualiseerd en aangevuld met verwerkingen waarbij de Gemeente Barneveld verwerker is in plaats van verwerkingsverantwoordelijke, zodat het register nog completer is. Eind december 2020 is de website volledig doorlopen op actualiteit en volledigheid, zodat geborgd is dat de juiste informatie verstrekt wordt.

4.4. Meldingen datalekken

IBD: Het jaar in cijfers
De IBD ontving het afgelopen jaar 3.845 vragen en meldingen rondom informatiebeveiliging en 715 privacyvragen. De IBD registreerde 175 incidenten met een hulp-, coördinatie- of ondersteuningsvraag van gemeenten en ontving hierover 750 inkomende telefoongesprekken. Eén maal werd het gemeentelijk responsnetwerk ingeroepen. Bij het incident in Hof van Twente in december, verleenden de IBD en experts van andere gemeenten ter plaatse assistentie. Behulpzame onderzoekers meldden 19 kwetsbaarheden onder de voorwaarden van responsible disclosure en kregen een plekje in onze hall of fame of een T-shirt als dank. De IBD verleende bij deze incidenten hulp variërend van bijvoorbeeld vertegenwoordiging in landelijk crisisoverleg bij de problemen rond Citrix tot advies over herstelwerkzaamheden en aanvullende maatregelen na een geslaagde phishingaanval. De IBD-CERT verstuurde 1.878 kwetsbaarheidsmeldingen.

De IBD organiseerde in 2020 meer dan 40 online bijeenkomsten zoals werkgroepen, intervisiebijeenkomsten, webinars en bespreekuren waarbij de nadruk lag op onderlinge gesprekken tussen de deelnemers. De website informatiebeveiligingsdienst.nl werd 134.103 maal bezocht en daar verschenen 72 nieuwe en bijgewerkte kennisproducten die samen met het totale aanbod maar liefst 94.115 keer werden gedownload. De meest gedownloade producten waren de BIO, de baselinetoets, de handreiking dataclassificatie en de standaard verwerkersovereenkomst. De IBD voert het beheer over het VNG privacyforum met meer dan 4.700 gemeentelijke deelnemers. Via de online DPIA-tool werden 70 nieuwe privacy-impactanalyses gemaakt op verschillende gemeentelijke processen en applicaties.

Cijfers Barneveld
In totaal zijn er in 2020 44 beveiligingsincidenten gemeld bij de Gemeente Barneveld. Nader onderzoek door de FG/PO/CISO wijst uit dat er 4 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 deze 4 gevallen is daarvan geen

sprake geweest. Ook heeft de AP geen waarschuwing gedaan of een dwangsom opgelegd aan de Gemeente Barneveld.

In de genoemde 4 gevallen zijn de betrokkenen geïnformeerd. Uit een analyse van de datalekken is bepaald dat er meer bewustwording moet worden gegeven over omgang met bedrijfsmiddelen. Daarnaast zijn er technische maatregelen getroffen om de gebruikers te ondersteunen.

4.5. Rechten van betrokkenen

In 2018 is het proces rond de rechten van betrokkenen verbeterd. In de privacyverklaring op de website is informatie opgenomen voor betrokkenen. De mogelijkheden tot het indienen van een verzoek of klacht zijn op de website voorzien. Er zijn formats opgesteld voor de ontvangstbevestiging, afwijzing en toewijzing van een verzoek. Ook is een stroomschema opgesteld hoe een verzoek behandeld moet worden. Er zijn in 2020 zes verzoeken binnengekomen. Van deze verzoeken zijn er twee niet in behandeling genomen, omdat het verzoek niet verder gespecificeerd is. Wat verder opvalt aan de andere verzoeken is dat drie 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 2020 geen klacht in verband met privacy ingediend.

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 heft gekregen dan het goed beveiligd thuiswerken. In 2021 zal dit weer opgepakt worden, nu iedereen gewend is geraakt aan het thuiswerken en weet met welke privacy en informatiebeveiligings- aspecten rekening gehouden moet worden.

4.7. Verwerkers en verwerkersovereenkomsten

In 2018 zijn de meeste verwerkersovereenkomsten afgesloten en in 2019 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 2020 is bij hoofdovereenkomsten die werden gewijzigd dan wel verlengd ook meteen de door VNG/ IBD verplicht gestelde verwerkersovereenkomst afgesloten, zodat er sprake is van een soort sterfhuisconstructie en 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 2020 in een geval afgeweken van de standaard en door VNG/IBD verplicht gestelde verwerkersovereenkomst. Dat is gedaan bij de Peutermonitor, november 2020, waarvan de bijlagen veel uitgebreider zijn dan de standaard. Artikel 7 iets anders, maar komt verderop terug in bijlagen, in diverse artikelen verwijzingen naar bijlagen. Of een kleine aanvulling op de artikelen. Doordat deze verwerkers-overeenkomst niet alleen voldoet aan de standaard artikelen en bijlagen, maar veel uitgebreider en gedetailleerder is omschreven, is daarmee akkoord gegaan.

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. Zo waren de FG en PO onder meer betrokken bij de aanschaf en implementatie van Suite4SD Regiemodule die per 1 januari 2021 gebruikt gaat worden, naast de gewone privacy vragen over de dagelijkse werkzaamheden en processen. Daarnaast heeft een jurist van Sociaal Domein een aantal handreikingen opgesteld over grondslagen en het verwerken van gegevens en deze ter advies voorgelegd aan de Privacy Officer.

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. Met Welzijn Barneveld vind ook incidenteel overleg plaats over privacy om kennis en ervaringen uit te wisselen.

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. Op 8 april 2020 heeft het MT de DPIA-rapportages voor kennisgeving aangenomen. Het college wordt hierover geïnformeerd middels dit jaarverslag.

In 2021 zullen er 7 DPIA's voor de onderstaande vakgebieden worden uitgevoerd, waarbij dit voor de meeste vakgebieden een herziening van de DPA uit 2018 betreft:

- AFAS (personeelsdossier)
- Blockchain wordt niet gedaan, omdat dit project niet uitgevoerd zal worden
- Innen vorderingen privaat en publiekrecht
- MDO-lokaal
- IBabs
- Evenementen
- Damocles
- Heffingen- en invorderingsadministratie

In 2020 uitgevoerde DPIA's:

- Suite4Sd Regie
- vroegsignalering schulden

In 2019 uitgevoerde DPIA's:

- Jeugdzorg
- Participatiewet (reintegratie)
- Milieupassensysteem
- Subsidie peuteropvang
- Camera's gemeentehuis
- Participatiewet (uitkering levensonderhoud, bijzondere bijstand, minimaregelingen)
- Beveiligingscamera's stations toiletten en fietsenstallingen
- Bodycams BOA's
- Kwijtschelding gemeentelijke belastingen
- Onderwijs - Leerlingenvervoer (melding en aanvraag)
- Onderwijs - Uitvoering Leerplichtwet en RMC- wet
- WMO - materiele hulp

- WMO - niet-materiele hulp
- IOAW- en IOAZ-uitkering
- Schuldhulpverlening
- Horeca aanvraag

In 2018 uitgevoerde DPIA's:

- Evenementen
- Damocles
- Rioolaansluitingen
- Woonurgentieverklaring
- BRS
- Vroegsignalering schuldhulp voorafgaand
- Heffingen- en invorderingsadministratie

De DPIA's vonden plaats aan de hand van de vragenlijst van de beroepsvereniging voor IT-auditors NOREA. 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 What's app 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 What's 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 What's 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 2020 op verschillende manieren gestalte gegeven.

Om medewerkers te laten weten dat we blij (Blij met Barneveld 😉) zijn dat ze zich goed bewust zijn van privacy en informatieveiligheid hebben we chocolaatjes uitgedeeld met logo Barneveld en een hartje met tekst privacy. Dit werd gewaardeerd. Verder lopen FG en PO regelmatig door de gangen en zetten dan kaartjes neer als iemand zijn beeldscherm niet heeft vergrendeld of zijn pasje heeft laten liggen… daarom waren de collega's op vrijdag 14 februari 2020 eerst wat argwanend, maar de chocolade werd zeer positief ontvangen als kleine blijk van waardering. Bij collega's die er niet waren die dag is de chocolade op het bureau gelegd. Ook is er een tekstje op intranet geplaatst. Vanaf medio maart is het door de coronapandemie en het thuiswerken niet meer mogelijk geweest om dergelijke rondes te lopen. In 2021 zal dat weer opgepakt worden, zodra er weer meer op kantoor gewerkt mag worden.

Door de coronapandemie zijn er meerdere initiatieven ontstaan die goed bedoeld zijn, maar strijdig met de wetgeving. Een voorbeeld hiervan is het verstrekken van telefoonnummers aan Boa's. Dit was bedoeld om ouders te kunnen bellen van jongeren als zij zich niet aan de corona-maatregelen zoals samenscholing en afstand houden. Strijdig met AVG, maar college heeft dit besluit genomen op 24 maart 2020.

Een ander voorbeeld is het betuigen van medeleven aan nabestaanden. Door Corona sterven veel mensen en door de Corona-maatregelen zijn uitvaarten anders geregeld. Men moet rekening houden met de 1,5 meter afstandsnorm en er mag maar een beperkt aantal mensen bij een uitvaart aanwezig zijn. Rouwverwerking en ondersteuning zijn daardoor anders. Vanuit de veiligheidsregio is een brief gestuurd hoe burgemeesters de nabestaande een hart onder de riem kunnen sturen. Een mooi initiatief en een gebaar van betrokkenheid vanuit de gemeente, maar wettelijk niet mogelijk (Wet BRP, AVG, etc.). Het college heeft dit besluit eind april 2020 genomen, maar uiteindelijk is de brief niet verstuurd.

Net als in 2018 en 2019, zijn er in 2020 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.

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 2021 voortgezet worden.

En vanuit informatieveiligheid blijft aandacht gevraagd worden voor het vergrendelen van het beeldscherm als de werkplek verlaten wordt. En het dan niet laten liggen van het toegangspasje. Ter voorkoming van het eenvoudig verschaffen van toegang tot vertrouwelijke gegevens, persoonsgegevens en bedrijfsgevoelige documenten en gegevens. Tevens is het van belang dat fysieke documenten veilig achter slot en grendel liggen en dat bezoekers tot aan de deur worden begeleid. Voor het thuiswerken geldt dit natuurlijk ook, omdat het niet de bedoeling is dan 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 zal dit verder opgepakt worden zullen waar nodig 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 2021

In de voorgaande hoofdstukken is aangegeven welke werkzaamheden in 2020 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 2021 worden de onderstaande acties opgepakt, waarover in het Jaarverslag FG 2021 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.
- 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.
- Aanvullende specifieke workshops voor vakgebieden, waarin veel (persoons)gegevens verwerkt worden. In overleg met de teamleiders bespreken welke vakgebieden daarvoor in aanmerking komen.
- 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 2021 een vervolg.
- Vastellen van het in 2020 geactualiseerde en herziene privacybeleid. Daarin zijn ook de verantwoordelijkheden van het lijnmanagement opgenomen.
- Vaststellen van het in 2020 opgestelde camerabeleid.
- In 2020 is uitgezocht welke actuele protocollen en procedures er op afdelingsniveau zijn of wenselijk zijn. Het opstellen of actualiseren van protocollen en procedures over de wijze van omgang met persoonsgegevens zullen in 2021 opgesteld gaan worden.
- Vaststellen van in 2020 opgesteld beleid voor toegang e-mail.
- Actiepunten zelfevaluatie oppakken
- Handreiking training Informatieveiligheid en Privacy actualiseren