Jaarverslag

Functionaris Gegevensbescherming 2023

Jaarverslag

Functionaris Gegevensbescherming 2023

Opdrachtgever:	gemeente Barneveld Bestuursondersteuning
Auteur:	Sascha Beekman, Functionaris Gegevensbescherming
Datum:	18 januari 2023 (versie v2)

Inhoud

1. MANAGEMENTSAMENVATTING

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 2023 heeft ondernomen om aan de vereisten van de Algemene Verordening Gegevensbescherming (AVG) en de Wet Politiegegevens (Wpg) te voldoen.

Het register van verwerkingen is geactualiseerd en er is voor de Wpg in 2022 een apart register opgesteld dat in 2023 verder is toegelicht. Daarnaast zijn er nieuwe of geactualiseerde verwerkersovereenkomsten afgesloten met 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.

Sinds de coronapandemie medio maart 2020 wordt door de meeste medewerkers zowel op kantoor als vanuit huis gewerkt. Thuiswerken brengt nieuwe mogelijkheden, maar ook risico's met zich mee op het gebied van privacy en informatiebeveiliging. Voor de risico's die thuiswerken met zich meebrengt is aandacht gevraagd.

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 2023 stond, evenals 2021 en 2022, 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 2023 aandacht besteed aan de evaluatie van de eerder gecommuniceerde aanbevelingen en te nemen maatregelen die zijn voortgekomen uit de uitgevoerde Data Protection Impact Assessments (DPIA's) om de verwerking van persoonsgegevens en onder andere de bewaartermijnen beter te borgen en na te leven.

In 2022 zijn een interne en externe audit uitgevoerd voor de Wet politiegegevens (Wpg). Op grond van de Wpg moet elk jaar een interne audit worden uitgevoerd en één keer per vier jaar een externe audit. De audits hebben betrekking op de

verwerking van politiegegevens door de buitengewone opsporingsambtenaren openbare ruimte en de leerplichtambtenaren. Uit de audits zijn een aantal verbeterpunten naar voren gekomen, die binnen een jaar doorgevoerd moeten worden. In 2023 zijn veel acties uit het Wpg verbeterplan opgepakt en uitgevoerd, waardoor de in november 2023 uitgevoerde externe audit over deze hercontrole er in heeft geresulteerd dat veel zaken zijn opgepakt en voldoen of bijna voldoen aan de in de audit gestelde normen. De nog openstaande zaken of de zaken waarin bijna of gedeeltelijk voldaan wordt aan de normen, worden in 2024 verder opgepakt en uitgewerkt. De rapportage over de hercontrole van de externe audit moest daarnaast voor 31 december 2023 zijn ingediend bij de Autoriteit Persoonsgegevens (AP), aan deze verplichting heeft de gemeente Barneveld voldaan.

2. WETTELIJK KADER

2.1 AVG Algemeen

In de 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 en 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 daarboven 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 Wet politiegegevens

Buitengewone opsporingsambtenaren (boa’s) die voor hun opsporingstaak persoonsgegevens verwerken, vallen onder de Wpg. Boa’s verwerken de politiegegevens onder beheer van hun werkgever en daarmee is de werkgever van de boa’s de verwerkingsverantwoordelijke. Voor de gemeente Barneveld geldt dat zij als werkgever boa’s openbare ruimte en leerplichtambtenaren in dienst heeft die bij het uitvoeren van hun taken politiegegevens verwerken. De Gemeente Barneveld is

daarom verantwoordelijk voor het toezicht op de naleving van de Wpg. In de Wpg is ook een auditverplichting opgenomen voor werkgevers van boa's.

- Interne Wpg-audit: elk jaar. Dat betekent dat de werkgever van die boa's verplicht is om elk jaar een interne Wpg-audit uit te voeren. De Gemeente Barneveld heeft in 2023 de privacy officer laten opleiden als interne auditor.
- Externe Wpg-audit: elke vier jaar. De werkgever moet elke vier jaar een externe Wpg-audit laten uitvoeren en de resultaten daarvan aan de Autoriteit Persoonsgegevens (AP) sturen.

2.3 Specifieke wetgevende ontwikkelingen, jurisprudentie en nieuwsberichten van de Autoriteit Persoonsgegevens

2.3.1 Wet gemeentelijke schuldhulpverlening (Wgs)

De gewijzigde 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 AP een handreiking[1] opgesteld met aandachtspunten. Hiermee moeten gemeenten en hulpverleners rekening houden om aan de privacywetgeving te voldoen.

2.3.2 Noodzaak van grootschalige dataverzameling in jeugdzorg niet aangetoond

Nieuwsbericht AP d.d. 14 december 2023[2]
Thema's: Gemeenten Gezondheidsgegevens gebruiken en delen

De AP heeft bezwaren tegen een wetsvoorstel dat leidt tot grootschalige dataverzameling in de jeugdzorg. Het voorstel zou onderzoek naar de beschikbaarheid van jeugdzorg binnen gemeenten mogelijk moeten maken. Maar onvoldoende duidelijk is waarom er bij zulk onderzoek veel privacygevoelige informatie van jongeren en hun ouders moet worden gedeeld.

Jeugdzorg beslaat in Nederland onder meer de kinderbescherming, hulp aan jongeren met psychische problemen en de reclassering. De bedoeling van het wetsvoorstel 'Verbetering beschikbaarheid jeugdzorg' is dat de Nederlandse Zorgautoriteit (NZa) gegevens kan gaan inzamelen voor onderzoek naar de beschikbaarheid van de jeugdzorg.

De NZa kan volgens het voorstel onder meer gezondheidsgegevens en strafrechtelijke gegevens van jongeren en hun ouders opvragen bij gemeenten en hulpverlenende instanties.

[1] https://www.autoriteitpersoonsgegevens.nl/themas/overheid/gemeenten/sociaal-domein
[2] https://www.autoriteitpersoonsgegevens.nl/actueel/noodzaak-van-grootschalige-dataverzameling-in-jeugdzorg-niet-aangetoond

2.3.3 Nationale Politie overtrad wet bij Schengen Informatiesysteem (SIS)

Nieuwbericht AP d.d. 20 december 2023[3]
Thema's: Europese informatiesystemen Politie, bijzondere opsporing en justitie

De Nationale Politie heeft met verwerkingen van persoonsgegevens in het Schengen Informatiesysteem (SIS) op een aantal punten de wet overtreden. Allereerst was de kwaliteit van de signaleringen in het SIS niet op orde. Daardoor stond er onjuiste of niet complete informatie over mensen in het systeem. Ook bleven signaleringen soms te lang bewaard. De overtredingen kwamen aan het licht na Europees onderzoek waaraan de AP deelnam.

Katja Mur, bestuurder AP: "Het SIS is een omvangrijk systeem, waarin veel informatie over mensen is opgeslagen. Vaak weten mensen zelf niet dat ze in het SIS staan. Zij zullen dan dus niet controleren of dat wel terecht is en of de informatie wel klopt. Dat legt een extra zware verantwoordelijkheid bij de gebruikers van het SIS. Want registratie kan grote impact hebben op mensen. Bijvoorbeeld een onterechte weigering aan de grens of een onnodige aanhouding."

De Nationale Politie nam in eerste instantie niet zelf maatregelen om de overtredingen in het SIS aan te pakken. De AP liet daarom aan de politie weten een last onder dwangsom te willen opleggen. Dat heeft de AP uiteindelijk niet hoeven doen, omdat de politie de overtredingen toen alsnog heeft beëindigd.

2.3.4 Gebruiken van persoonsgegevens uit overheidsdata

De AP adviseert het voorstel voor een wijziging van de Wet hergebruik van overheidsinformatie aan te passen[4]. Het voorstel, waarin het kabinet overheidsinstellingen aanmoedigt overheidsdata, inclusief persoonsgegevens, beschikbaar te stellen voor hergebruik, stelt onvoldoende grenzen. Met het risico dat persoonsgegevens worden gedeeld zonder toestemming of medeweten van de mensen om wie het gaat.

Het wetsvoorstel moet ervoor zorgen dat zoveel mogelijk overheidsdata beschikbaar worden gesteld, bijvoorbeeld voor onderzoek, maar ook voor commercieel gebruik. Die data moeten volgens het voorstel ook doorzoekbaar zijn met software en te combineren zijn met andere data. Overheidsinstellingen worden verzocht informatie openbaar te maken, tenzij zij zelf inschatten dat dat niet kan.

In haar advies aan het kabinet pleit de AP ervoor om in de wet op te nemen dat hergebruik van persoonsgegevens in openbare registers in principe verboden is. En vervolgens in regels vast te leggen wanneer welke persoonsgegevens wél voor

[3] https://www.autoriteitpersoonsgegevens.nl/actueel/nationale-politie-overtrad-wet-bij-schengen-informatiesysteem-sis
[4] AP: stel grenzen aan opnieuw gebruiken van persoonsgegevens uit overheidsdata | Autoriteit Persoonsgegevens

hergebruik beschikbaar mogen worden gesteld, en dus een uitzondering zijn op dat verbod. In de regels moet ook rekening worden gehouden met de vrijheid van mensen om hun gegevens toch voor hergebruik beschikbaar te laten stellen.

2.3.4 AP: centrale database paspoortgegevens groot risico

Nieuwsbericht AP d.d. 30 januari 2023[5]
Thema's: Datalekken Beveiliging van persoonsgegevens Biometrie Paspoort en identiteitskaart Gemeenten

Het kabinet wil een centrale database maken met alle persoonsgegevens die mensen aanleveren voor een paspoortaanvraag, zoals vingerafdrukken, handtekeningen en pasfoto's. Zo'n database met gegevens van heel veel Nederlanders brengt grote privacy risico's mee die het kabinet niet goed meeweegt. Ook kan er onduidelijkheid ontstaan over wie verantwoordelijk is voor de veiligheid van de gegevens. De AP adviseert dan ook de plannen grondig aan te passen of anders in te trekken.

2.4 Toezichtskader AP: ontwikkelingen en gevolgen

De AP heeft in eind december 2023 haar toezichtkader voor het jaar 2024 gepubliceerd. In het 'Jaarplan 2024'[6] geeft de AP haar prioriteiten aan voor de komende jaren. Toezicht houden betekent ook keuzes maken. Het toezichtveld van de AP wordt namelijk steeds groter en de middelen zijn beperkt. Daarom richt de AP zich op de grootste risico's voor burgers en samenleving. De bescherming van publieke belangen staat altijd voorop. Zoals gelijke behandeling, persoonlijke autonomie en de controleerbaarheid van macht.

Focusgebieden
De AP legt in 2024 in het toezichtwerk extra nadruk op vijf focusgebieden:

- Algoritmes en AI
- Big Tech
- Vrijheid en Veiligheid
- Datahandel
- Digitale Overheid

Algoritmes & AI
Algoritmes en AI zijn niet meer weg te denken uit onze samenleving. Algoritmes bieden een hoop kansen. Bijvoorbeeld voor het bedrijfsleven, de wetenschap en de medische wereld. Tegelijkertijd kan door onverantwoorde ontwikkeling of inzet van algoritmes grote schade ontstaan. Onjuiste data of data die gebaseerd zijn op foutieve aannames, kunnen zowel bij de overheid als bij bedrijven grote risico's voor burgers met zich meebrengen. Zoals uitsluiting of discriminatie. Dat wil de AP voorkomen door

[5] https://www.autoriteitpersoonsgegevens.nl/actueel/ap-centrale-database-paspoortgegevens-groot-risico
[6] https://www.autoriteitpersoonsgegevens.nl/documenten/ap-jaarplan-2024

de risico's in kaart te brengen en handvatten te bieden voor veilig en verantwoord gebruik van algoritmes en AI.

Wat doet de AP in ieder geval in 2024?
• AP geeft prioriteit aan klachten, datalekken en onderzoeken die over algoritmes en AI gaan, zodat de AP zicht krijgt op waar en waarom dingen misgaan.
• Signaleren en analyseren van overkoepelende risico's van algoritmes die in meerdere sectoren spelen. Twee keer per jaar publiceert de AP de Rapportage Algoritmerisico's Nederland (RAN).
• De AP geeft uitleg over de risico's van algoritmes en communiceert de 'best practices' over hoe algoritmes verantwoord zijn in te zetten.
• De AP werkt samen met andere toezichthouders om ervoor te zorgen dat het toezicht op algoritmes goed is afgestemd.

Big Tech
De invloed van grote Tech bedrijven blijft groeien. Een klein aantal bedrijven heeft hierdoor veel macht. Omdat deze bedrijven ook veel persoonlijke gegevens in handen hebben, kunnen ze mensen beïnvloeden. Bijvoorbeeld door nepnieuws en politieke targeting op basis van profielen. Dat vormt een bedreiging voor onze democratie en samenleving. Om ervoor te zorgen dat grote Tech bedrijven zich aan de AVG houden, werkt de AP veel samen met andere Europese toezichthouders. En treedt de AP hard op als dat nodig is.

Wat doet de AP in ieder geval in 2024?
• De AP doet (internationaal) onderzoek naar overtredingen door grote Tech bedrijven. Klachten over deze bedrijven behandelt de AP met voorrang. Voor het onderzoek kan de AP speciale instrumenten inzetten.
• Samen met de andere Europese toezichthouders draagt de AP eraan bij dat grote Tech bedrijven alleen generatieve AI-modellen ontwikkelen en aanbieden die voldoen aan de wet en veilig zijn voor mensen, nu en in de toekomst.
• De AP werkt samen met haar Europese collega's aan innovatieve manieren om het toezicht op Big Tech effectiever vorm te geven, om zo de grondrechten van burgers nog beter te beschermen.

Vrijheid & veiligheid
Vrijheid en veiligheid kunnen op gespannen voet met elkaar staan. Om de veiligheid te vergroten, moeten er soms maatregelen worden genomen die de vrijheid beperken. Omdat vrijheid en veiligheid voor mensen beide van fundamenteel belang zijn, moet een zorgvuldige afweging worden gemaakt tussen meer van het een en minder van het ander. De AP let bij de verwerking van persoonsgegevens extra op een verdedigbare balans tussen vrijheid en veiligheid.

Wat doet de AP in ieder geval in 2024?
• De AP doet onderzoek naar en houdt toezicht op grote Europese informatiesystemen en databases die worden gebruikt voor het beschermen van de buitengrenzen van het Schengengebied.
• Bij de inzet van nieuwe, risicovolle technologieën in het veiligheidsdomein adviseert de AP gevraagd en ongevraagd over wat wel en niet mag, om zo te voorkomen dat grondrechten in het geding komen.
• Het gebruik van gezichtsherkenningstechnologie om de veiligheid te vergroten brengt ook grote risico's voor burgers met zich mee. De AP besteedt hier extra aandacht aan en geeft praktische handvatten voor veilig gebruik.

Datahandel
De steeds meer gedigitaliseerde ('slimme') producten en diensten die er gebruikt worden, creëren veel waardevolle data. Met als gevolg dat er ook steeds meer ongeoorloofde (door)verkoop plaatsvindt van persoonsgegevens. Niet alleen in Nederland, maar ook internationaal. Dat moet een halt toegeroepen worden.

Wat doet de AP in ieder geval in 2024?
• De AP start een meerjarenproject dat het ongeoorloofd online volgen van mensen, bijvoorbeeld met cookies, op verschillende fronten aanpakt.
• De AP geeft prioriteit aan onderzoek naar klachten en datalekmeldingen die een duidelijke link hebben met datahandel.
• De AP zet extra in op voorlichting en communicatie over naleving op het gebied van datahandel. Zo zorgen ze ervoor dat bedrijven zich aan de wet houden en burgers geen schade oplopen.

Digitale overheid
De overheid beschikt over veel – vaak gevoelige – persoonsgegevens van Nederlandse burgers en maakt hier veel gebruik van. Het risico dat burgers in de knel komen is groot als de overheid verkeerd omgaat met hun persoonsgegevens. Bovendien heeft de overheid een voorbeeldfunctie als het gaat om de verantwoorde omgang met persoonsgegevens. Om ervoor te zorgen dat overheidsorganisaties veilig omgaan met persoonsgegevens schenkt de AP hier extra aandacht aan en deelt de AP haar kennis hierover.

Wat doet de AP in ieder geval in 2024?
• De AP reserveert extra capaciteit om onderzoek te doen naar overheden en uitvoeringsorganisaties die persoonsgegevens van burgers gebruiken in algoritmes.
• De AP besteedt opnieuw aandacht aan het delen van gegevens tussen verschillende onderdelen van de overheid en andere organisaties. Daarnaast geeft de AP aandacht aan de risico's van het gebruik van algoritmes bij de overheid, zoals discriminatie.
• De AP deelt gevraagd en ongevraagd kennis over gegevensuitwisseling in het sociaal domein en over privacy waarborgen bij fraudebeleid en schuldhulpverlening.

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 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 mei 2023 in werking getreden herziene Privacybeleid. 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 2023:

- In 2023 zijn de uit de in 2022 uitgevoerde Data Protection Impact Assessments (DPIA's) voortvloeiende acties opgepakt en uitgevoerd. Tevens zijn de DPIA's in het Sociaal Domein herzien.
- Het Register van Verwerkingen is in 2023 geactualiseerd en er is in 2022 een register voor de Wpg opgesteld dat in 2023 verder is toegelicht.
- Begin januari 2023 is aan de hand van het IBD borgingsdocument de borging van privacy en informatiebeveiliging beoordeeld en zijn de resultaten geëvalueerd ten opzichte van het jaar daarvoor. De daaruit voortkomende acties zijn vervolgens in 2023 opgepakt [Zie verder bij 3.5]. In januari 2024 zal aan de hand van het vernieuwde borgingsdocument versie 3.0 van IBD de borging wederom worden beoordeeld. De acties die daaruit voortkomen worden vervolgens in 2024 opgepakt en uitgevoerd.
- Voor de Wpg is een interne en externe audit uitgevoerd en naar aanleiding daarvan is begin 2023 een verbeterplan opgesteld dat op 2 maart 2023 is vastgesteld door het college. De punten uit dit verbeterplan zijn in 2023 opgepakt en dat heeft geresulteerd in een sterk verbeterde audit-uitkomst. De nog openstaande of deels gerealiseerde verbeterpunten worden in 2024 verder opgepakt en uitgevoerd.

3.3 Verantwoording Privacy Officer

Overzicht uitgevoerde werkzaamheden in 2023:

DPIA's	In 2023 zijn een aantal DPIA's uitgevoerd op risicovolle processen, waaronder de overgang naar een nieuw systeem voor het telefonie- en contactcentrum en een aantal processen in het sociaal domein. Daarnaast is een procesbeschrijving gemaakt voor de uitvoering van DPIA's.

Privacybeleid	Het privacybeleid is geactualiseerd en hierin is ook de Wet politiegegevens meegenomen.
Bewustwording privacy en informatiebeveiliging	- Er zijn trainingen voor (nieuwe) medewerkers verzorgd. - Periodiek is een nieuwsbericht op intranet gezet.
Wet politiegegevens	Door de PO is, in samenwerking met de inhoudelijke collega's een interne audit uitgevoerd op de verwerking van politiegegevens. Daarnaast is een hercontrole uitgevoerd door een externe auditor, deze is door de PO gecoördineerd.
Privacy en Publiekszaken	In overleg met Publiekszaken is ondersteuning geboden bij privacyvraagstukken (verstrekken gegevens uit de BRP).
Onderhouden register van verwerkingen	Nieuwe processen worden toegevoegd en wijzigingen in processen worden in het register doorgevoerd.
Ondersteunen bij ontwikkelingen in de organisatie	Bij ontwikkelingen in de organisatie is de privacyregelgeving meegenomen en neemt waar nodig de PO deel aan (implementatie) projecten.
Inzageverzoeken	De meeste inzageverzoeken hebben betrekking op het sociaal domein en publiekszaken en zijn door de Privacy Officer afgehandeld in samenwerking met een betrokken collega.
Datalekken	De procedure voor de behandeling van datalekken (AVG en Wpg) is aangepast. Inbreuken in verband met privacy zijn geregistreerd. Datalekken zijn gemeld bij de AP.
Overige werkzaamheden	Naast de hierboven genoemde werkzaamheden zijn door de PO de volgende werkzaamheden verricht: - Toetsen/ opstellen verwerkersovereenkomsten - Toetsen/ opstellen convenanten - Behandelen privacyvraagstukken - Signaleringsfunctie in organisatie - Sparringpartner voor de organisatie -

3.4 Verantwoording CISO

Overzicht van uitgevoerde werkzaamheden in 2023:

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. - Ter versterking van bewustwording is periodiek een nieuwsbericht op intranet gezet. Maandelijks krijgen alle nieuwe medewerkers een basistraining Privacy en Informatiebeveiliging.
Zelfevaluatie BRP/PNIK	Jaarlijks draagt de gemeente verantwoording af over informatiebeveiliging rond BRP / Pnik.
Zelfevaluatie ENSIA	Jaarlijks draagt de gemeente verantwoording af over informatiebeveiliging door middel van ENSIA (Eenduidige Normatiek Single Information Audit). Hierin vallen onder andere BAG, BGT, DigiD, Suwinet. Daarbij worden DigiD, Suwinet en de ENSIA-verantwoording getoetst door een externe RE/RA auditor.
BIO	Controleren en evalueren van de huidige set maatregelen.
SIEM/SOC	Er is een Proof Of Concept implementatie gedaan van een extern Security Operations Center dat 24x7 de IT-omgeving van de gemeente bewaakt. Besloten is hiervoor structureel budget aan te vragen.
Informatie-beveiliginsbeleid	Er is een nieuw strategisch informatiebeveiligingsbeleid geschreven dat naar verwachting in januari 2024 wordt vastgesteld.

3.5 Borging

De VNG en IBD hebben samen begin 2021 een vernieuwd borgingsdocument opgesteld, dat bestaat uit 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. O ziet op organisatiemaatregelen en P ziet op procesmaatregelen. De vragen zijn opgesplitst in 7 onderdelen: beleid, processen, organisatorische inbedding, rechten van betrokkenen, samenwerking, beveiliging en verantwoording.

Voor het jaar 2023 is in januari 2023 de control vragenlijst uitgevoerd door de PO, CISO en FG. 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.

Verder is bij nog niet iedere applicatie logging en monitoring ingeregeld of zijn zaken niet automatisch maar alleen handmatig te wijzigen. De oorzaak hiervan ligt soms in het feit dat het om oudere applicaties gaat waarbij dat lastiger is in te regelen. Bij alle applicaties die onlangs zijn aangeschaft of nog worden aangeschaft wordt vooraf al een programma van eisen opgesteld, zodat er sprake is van privacy by design en privacy by default. Hierdoor wordt dan niet geheel aan de norm voldaan of is het volwassenheidsniveau minder hoog, omdat de norm en het volwassenheidsniveau over de gehele gemeente wordt gemeten.

Een aantal zaken die volgens de beoordeling in januari 2023 op gedeeltelijk staan, zijn in 2023 in de actualisering van beleid en de opstelling van nieuw beleid meegenomen. Het privacybeleid is een voorbeeld van een herzien beleid waarin meerdere zaken uit het resultaat van de borging uit januari 2023 zijn meegenomen, waardoor deze bij de beoordeling van de borging in januari 2024 als resultaat ‘geregeld’ of ‘is aan voldaan’ zullen krijgen. Zo wordt jaarlijks een deel van de nog openstaande zaken of zaken die op niet of gedeeltelijk aan voldaan staan opgepakt. Overigens kan opgemerkt worden dat een 100% score nooit te garanderen is, omdat privacy & security vakgebieden zijn die continue in beweging zijn.

In de loop van 2023 is de IBD met een vernieuwd borgingsdocument (versie 3.0) gekomen. In januari 2024 zal dit document gebruikt worden voor het maken van een nieuwe beoordeling van de borging van de privacy en security in de gemeente Barneveld, zodat daar in 2024 vervolgens opvolging aan gegeven kan worden.

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 gegevensuitwisseling tussen verschillende domeinen en afdelingen.

Zowel in 2021, 2022 als in 2023 heeft een herziening plaatsgevonden van het privacybeleid, waarin bij de beleidsherziening in 2023 tevens de Wpg is opgenomen. Het nieuwe (herziene) privacybeleid is op 18 april 2023 vastgesteld door het college en is op 1 mei 2023 in werking getreden. De raad is hierover geïnformeerd en ook op de website van de Gemeente Barneveld is hier aandacht aan besteed.

4.2 Thuiswerken

In de jaren 2020 tot en met 2022 waren er landelijk maatregelen afgekondigd ter bestrijding van Covid-19. Bij de Gemeente Barneveld zijn toen ook lokaal maatregelen getroffen. Een daarvan was het thuiswerken voor alle medewerkers, tenzij dat niet mogelijk was vanwege de aard van de werkzaamheden (zoals (deel) publiekszaken, afvalophaaldienst, groenvoorziening e.d.). Ook in 2023 is het hybride werken (deels thuis, deels op kantoor werken) veel toegepast en dat zal ook de komende jaren zo blijven, omdat gebleken is dat dit prima werkt. Een belangrijk punt daarbij is dat medewerkers goed in hun agenda bijhouden waar en wanneer ze bereikbaar zijn. Daarbij is ook in 2023 aandacht gevraagd voor de risico’s die thuiswerken met zich meebrengt, aangezien thuiswerken niet alleen nieuwe mogelijkheden biedt, maar ook risico’s met zich meebrengt op het gebied van privacy en informatiebeveiliging.

Er is benadrukt dat de regels van privacy en informatiebeveiliging in acht genomen moeten worden. 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, ook middels de verplichte workshops. Daarbij zijn medewerkers erop geattendeerd dat ze met vertrouwelijke gegevens en informatie werken. De thuiswerkregeling is in 2023 geactualiseerd en onder de aandacht gebracht van alle medewerkers.

4.3 Wpg- audit

4.3.1 Audit over 2021 en 2022

Op grond van de Wpg moet elk jaar een interne audit worden uitgevoerd en één keer per vier jaar een externe audit. In 2022 zijn er zowel een interne als een externe audit uitgevoerd voor de Wpg over het jaar 2021. De audits hebben betrekking op de verwerking van politiegegevens door de buitengewone opsporingsambtenaren openbare ruimte en de leerplichtambtenaren. Uit de audits zijn een aantal verbeterpunten naar voren gekomen, die binnen een jaar doorgevoerd moeten worden. Hiervoor is begin 2023 een verbeterplan opgesteld en de actiepunten daarin zijn opgepakt en uitgevoerd.

Uitvoering steekproef

Zowel in het domein openbare ruimte als voor het domein onderwijs (leerplicht) zijn steekproefsgewijs controles uitgevoerd op zowel de logging van zaken in de applicaties als inhoudelijk op de processen-verbaal (beide domeinen) en Halt-verwijzingen (bij leerplicht). Getoetst is of wordt voldaan aan de in het Wpg controleprotocol vastgelegde criteria. Hierdoor is inzichtelijk of de politiegegevens op de juiste wijze en voldoende zorgvuldig worden verwerkt. Van de gehouden controles zijn rapportages met bevindingen opgesteld. Daaruit zijn leerpunten voortgekomen die direct of vanaf het volgende schooljaar toegepast gaan worden om beter aan de Wpg te voldoen.

Hercontrole audit 2021 en 2022

In november 2023 heeft een hercontrole plaatsgevonden over de voorgaande jaren. Deze is door de externe partij uitgevoerd die ook de eerdere externe audit heeft uitgevoerd. De auditor heeft de Gemeente Barneveld gecomplimenteerd dat er zoveel zaken opgepakt en uitgevoerd zijn, waardoor het auditresultaat nu op veel punten als (deels) aan voldaan kan worden beschouwd. De nog openstaande zaken of de zaken die gedeeltelijk voldoen worden verder opgepakt en uitgevoerd in 2024.

De rapportage over de externe audit over de hercontrole moest daarnaast voor 31 december 2023 zijn ingediend bij de Autoriteit Persoonsgegevens (AP), aan deze verplichting heeft de gemeente Barneveld voldaan.

4.3.2 Audit over 2023

In 2023 heeft ook de interne audit over 2023 plaatsgevonden. Vanwege het opgestelde en actief opgepakte verbeterplan wordt bij de meeste zaken voor 2023 daardoor, net als het geval is bij de audit over de hercontrole, voldaan of (deels) voldaan aan de normen. De nog openstaande zaken of de zaken die gedeeltelijk voldoen worden verder opgepakt en uitgevoerd in 2024.

4.4 Register van verwerkingen

In 2023 is het register van verwerkingen geactualiseerd. Bij alle verwerkingen die in het register zijn opgenomen, worden de bewaartermijnen gehanteerd zoals deze door de VNG zijn vastgesteld in de "Selectielijst 2020".

In 2022 zijn nieuwe verwerkingen in het register opgenomen en gewijzigde verwerkingen zijn aangepast. Ook is de nieuwe organisatiestructuur in het register opgenomen. Daarnaast zijn in 2022 in het register verwerkingen aangepast dan wel toegevoegd, om een duidelijk onderscheid te maken tussen verwerkingen op grond van de AVG en verwerkingen op grond van de Wpg. Deze Wpg verwerkingen zijn in 2023 aan de hand van het verbeterplan Wpg verder uitgewerkt of nader toegelicht.

4.5 Meldingen datalekken

4.5.1 Cijfers AVG

In totaal zijn er in 2023 32 AVG beveiligingsincidenten gemeld bij de Gemeente Barneveld. Hiervan is één incident gemeld bij 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 2023 is daarvan geen sprake geweest. Ook heeft de AP geen waarschuwing gedaan of een dwangsom opgelegd aan de Gemeente Barneveld.

Bij geen enkel incident waren de risico's dermate hoog dat het verplicht was om een melding aan de betrokkenen te doen. Vanuit klantgerichtheid zijn betrokkenen echter in een aantal gevallen wel geïnformeerd. 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.

4.5.2 Cijfers Wpg

In 2023 zijn er geen Wpg beveiligingsincidenten gemeld bij de Gemeente Barneveld.

De procedure meldplicht datalekken is in 2023 geactualiseerd en de Wpg is daar nu ook in opgenomen, omdat de procedure voorheen alleen zag op de AVG.

4.6 Rechten van betrokkenen

4.6.1 AVG verzoeken

Er zijn in 2023 20 verzoeken binnengekomen. Alle deze verzoeken waren verzoeken tot inzage. De meeste verzoeken zijn toegewezen en hebben betrekking op het Sociaal Domein en publiekszaken.

Oorspronkelijk zijn in 2023 meer verzoeken ingediend, maar na telefonisch contact blijkt veelvuldig dat een verzoek niet als inzageverzoek is bedoeld, maar meer een informatievraag is. Vaak gaat het dan om vragen die betrekking hebben op publiekszaken of informatie die personen zelf kunnen opzoeken. Na telefonisch contact

blijkt dan geen sprake te zijn van een inzageverzoek en wordt de vraag indien nodig doorgezet naar de juiste afdeling. In 2023 zijn geen privacy klachten ingediend.

4.6.2 Wpg verzoeken

Er zijn in 2023 geen verzoeken gedaan op grond van de Wpg waarin betrokkenen een beroep op hun rechten deden.

4.7 Bewaartermijnen

In 2019 zijn digitale bezemdagen georganiseerd in verschillende teams en zijn teams actief gewezen op het opschonen van mappen op netwerkschrijven en in e-mailboxen. Door de coronapandemie is er door de meeste medewerkers veel thuis gewerkt, waardoor het goed beveiligd thuiswerken meer prioriteit heeft gekregen dan het digitaal bezemen. Eind 2021 is het digitaal bezemen weer door enkele teams opgepakt en het was de bedoeling om dit in 2023 ook weer onder de aandacht te brengen, maar de teamleiders en CT willen daarover nog met elkaar afstemmen welke periode het best werkbaar is. Het digitaal bezemen schuift daarom door naar 2024.
Inmiddels is iedereen gewend geraakt aan het thuiswerken en weet men met welke privacy- en informatiebeveiligingsaspecten rekening gehouden moet worden.

4.8 Verwerkers en verwerkersovereenkomsten

Van alle leveranciers waarmee een verwerkersovereenkomst is afgesloten is een actueel overzicht. Bestaande verwerkers hebben niet gerapporteerd over incidenten. 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 voor een inhoudelijke check.

Bij het afsluiten van verwerkersovereenkomsten met leveranciers wordt standaard de model verwerkersovereenkomst gehanteerd die verplicht is gesteld door de VNG/IBD. Dit is in 2023 bij alle verwerkersovereenkomsten gebeurd. Wel is bij enkele verwerkersovereenkomsten artikel 7 van de overeenkomst aangepast. Artikel 7 verwijst voor het opschonen van gegevens naar de hoofdovereenkomst. Als dat opschonen niet in de hoofdovereenkomst is geregeld, dan wordt dit in de verwerkersovereenkomst geregeld.

4.9 Privacy in het Sociaal Domein

Tussen de sector Samenleving (voorheen 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 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 teams van het Sociaal Domein.

Wat betreft leerplicht worden er behalve AVG persoonsgegevens ook Wpg politiegegevens verwerkt. Met de (bestaande) ketenpartners zijn al eerder overeenkomsten afgesloten, waarin de bescherming van die gegevens geborgd is.

4.10 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.

4.11 Data Protection Impact Assessments

In 2023 zijn er DPIA's voor de onderstaande processen uitgevoerd:

1.	KCC	Telefonie en contactcentrum	Nieuwe/gewijzigde verwerking
2.	Leefgeld Oekraïne	Leefgeld Oekraïne	Nieuwe/gewijzigde verwerking
3.	Plinkr Hub	Plinkr Hub	Nieuwe/gewijzigde verwerking
4.	Beveiligingscamera's	Beveiligingscamera's stations toiletten en fietsenstallingen	Periodieke herziening
5.	Horeca-aanvragen	Horeca-aanvraag	Periodieke herziening
6.	WMO	WMO – materiële hulp	Periodieke herziening
7.	WMO	WMO – niet-materiële hulp	
8.	Participatiewet	IOAW- en IOAZ-uitkering	Periodieke herziening
9.	Participatiewet	Participatiewet (uitkering levensonderhoud, bijzondere bijstand)	
10.	Participatiewet	Participatiewet – re-integratie	
11.	Jeugdzorg	Jeugdzorg	Periodieke herziening
12.	Inburgering	Uitvoering wet inburgering	Nieuwe/gewijzigde verwerking

In 2024 zullen er in ieder geval DPIA's voor de onderstaande processen worden uitgevoerd, waarbij dit voor de meeste processen een herziening en verdieping van de DPIA uit 2019 of 2020 betreft:

1.	Processen PGax	Processen PGax (verwarde personen/signalen ondermijning)	Nieuwe/gewijzigde verwerking
2.	Anonimiseren van gegevens Woo	Anonimiseren van gegevens Woo	Nieuwe/gewijzigde verwerking
3.	Participatiewet	BBZ	Periodieke herziening
4.	Schuldhulpverlening	Vroegsignalering schuldhulp voorafgaand	Periodieke herziening
		Schuldhulpverlening	
5.	Jeugdzorg	MDO-lokaal	Periodieke herziening

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 proces wordt een rapportage opgesteld met bevindingen, conclusies en aanbevelingen.

In de in 2023 uitgevoerde DPIA's komen – samengevat – de volgende risico's naar voren:

- In werkinstructie opnemen in welke situatie welke gegevens verzameld mogen worden;
- Bewaartermijnen in applicaties goed laten inregelen door leverancier;
- Informeren betrokkenen door dit duidelijker in gesprekken mee te nemen en de informatie op de website te updaten en informatieborden aanpassen
- Onderzoeken en vastleggen in welke situaties Whatsapp wel en wanneer niet gebruikt kan/mag worden;
- Beoordelen of grondslag passend is;
- Periodieke beoordeling camera's op noodzakelijkheid;
- Beleid opstellen voor logging en monitoring of nog te maken werkafspraken;
- Opslaan van documenten in Teams werkt niet naar behoren, waardoor schaduwarchief is ontstaan in Onedrive. Opslaan en bewaren van gegevens in Outlook is niet de juiste werkwijze. In geen geval dubbele administraties meer bijhouden in teams, onedrive, outlook naast gebruik van Zaaksysteem of vak applicatie. Dit moet opgeschoond en beëindigd worden en de documenten moeten in het Zaaksysteem of in de vak applicatie opgeslagen worden;
- Verwerkersovereenkomsten actualiseren en/of afsluiten;

- Samen met leverancier onderzoeken of het mogelijk is om database (beter) te versleutelen;
- Toevoegen/aanpassen van verschillende verwerkingen in het register van verwerkingen en op website;
- Persoonsgebonden accounts gaan gebruiken in plaats van een groepsaccount door het aanpassen van de autorisaties;
- Ieder kwartaal monitoren gegevens om ongewenst gedrag of onrechtmatig gebruik snel inzichtelijk te hebben;
- Functionaliteit voor het downloaden van gegevens en documenten buiten de VDI uitzetten;
- Bij het maken van analyses gebruik maken van geanonimiseerde gegevens;
- Maken werkafspraken met ketenpartners en deze schriftelijk vastleggen.

De volgende maatregelen zijn reeds genomen:
- Onjuiste opslag/creëren van schaduwarchief in Onedrive/Outlook is direct opgepakt en die wijze van opslag is beëindigd. De gegevens worden voortaan in de vak applicatie opgeslagen of direct in het Zaaksysteem opgeslagen;
- De informatiebordjes op de stations waaruit blijkt dat gebruik gemaakt wordt van beveiligingscamera's zijn aangepast;
- De periodieke controle van beveiligingscamera's op noodzakelijkheid is direct opgepakt;
- Het actualiseren van de website over het informeren van betrokkenen in de verschillende vakgebieden is direct opgepakt. Ook het informeren van betrokkenen in gesprekken is direct in de werkwijze aangepast;
- Functionaliteit voor het downloaden van gegevens en documenten buiten de VDI is uitgezet;
- Bij het maken van analyses wordt inmiddels gebruik gemaakt van geanonimiseerde gegevens.

Verder zijn er afspraken gemaakt over de termijn waarop andere maatregelen worden genomen. Denk hierbij aan het doorvoeren van de wijzigingen in de werkwijze in de werkinstructies en het opnemen van contact met de leverancier om de bewaartermijnen goed in te regelen of het maken van afspraken met ketenpartners. Deze te nemen maatregelen kosten meer tijd, omdat er vaak meer interne en externe partijen bij betrokken zijn.

4.12 Bewustwording

Net als in voorgaande jaren, zijn er in 2023 workshops over Privacy en Informatiebeveiliging gehouden. Deze workshop is verplicht voor alle nieuwe medewerkers en wordt sinds 2023 in kleinere groepen gehouden voor een betere interactie. Belangrijk voor de bewustwording is ook de bekendheid en benaderbaarheid van de PO om als vraagbaak te fungeren. Hiervan is en wordt veel gebruik gemaakt.

4.13 Overige zaken

Er is in 2023 gesignaleerd dat er een keer sprake is geweest van een onjuist gebruik van persoonsgegevens en/of vertrouwelijke gegevens. Bij de benoeming van een lid van de bezwarenadviescommissie is verzocht om het curriculum vitae (cv) van de te benoemen persoon als informatie toe te voegen aan het benoemingsbesluit. Hierover heeft de FG geadviseerd dit niet toe te staan, omdat het benoemingsbesluit slechts een formaliteit is, omdat er al een selectie- en benoemingscommissie over de geschiktheid van de kandidaat heeft geoordeeld.

Verder is in 2023 geconstateerd dat het "Beleid toegang mailbox" is verouderd en dat dit moet worden geactualiseerd. Dit kwam aan het licht op het moment dat toegang tot een mailbox werd verlangd van een vertrokken medewerker en een keer van een langdurig zieke medewerker, omdat bepaalde afspraken in outlook te vinden waren en nog geformaliseerd moesten worden. In deze specifieke gevallen is eenmalig kortdurend toegang verleend. In 2024 wordt dit beleid herzien en geactualiseerd, zodat ook bij dit soort situaties vastligt hoe omgegaan wordt met het wel of niet verlenen van toegang tot andermans mailbox en aan wie die bevoegdheid toegekend wordt en wie een dergelijke aanvraag moet beoordelen en goedkeuren, voordat ICT de gevraagde actie uitvoert.

4.14 Te verwachten ontwikkelingen wet- en regelgeving

Ook in 2023 en 2024 zijn er wetswijzigingen te verwachten, waarin gegevensverwerking voorkomt.

Verzamelwet Gegevensbescherming

De Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) is geactualiseerd en is in februari 2023 in werking getreden. De UAVG is een verlengstuk van de AVG. Verschillende andere wetten verwijzen ook naar de UAVG en deze wetten worden ook aangepast om ze beter op de AVG en de UAVG af te stemmen.

De wijzigingen zijn:

- Meer rechten voor kinderen tussen 12 en 16 jaar.
- Aanpassing aan de uitleg van het begrip strafrechtelijke persoonsgegevens.
- Grondslag voor accountants en curatoren om bijzondere persoonsgegevens en/ of strafrechtelijke persoonsgegevens te verwerken.
- Het gebruik van biometrische gegevens met het doel om toegang te krijgen tot bepaalde plaatsen, diensten, informatiesystemen, etc.
- Bij pensionering of overlijden van een hulpverlener wordt de overdracht van dossiers naar een andere hulpverlener, die ze gedurende de wettelijke bewaartermijn bewaart, beter geregeld.

Algoritmeregister

Sinds december 2022 zijn ruim honderd algoritmes die de overheid gebruikt in een online-register samengebracht in het Algoritmeregister[7]. De nieuwe site moet zorgen

[7] https://algoritmes.overheid.nl/nl

voor meer transparantie over de algoritmes die overheden inzetten. Ministeries, gemeenten en andere takken van de overheid kunnen hun algoritmes delen op het Algoritmeregister, maar dat is nog niet verplicht. De Tweede Kamer wil wel dat dit gebeurt. De verwachting is dat een dergelijke verplichting op zijn vroegst in 2024 van kracht wordt. In de Europese Unie is ook regelgeving in de maak die verplicht om algoritmes met een 'hoog risico' publiek inzichtelijk te maken.

Het Algoritmeregister staat los van de (Europese) AI verordening, maar heeft daar wel een verband mee. Na drie dagen intense onderhandeling, hebben het Europees Parlement en de Raad van de Europese Unie een voorlopig politiek akkoord bereikt over een serie aan uniforme voorwaarden voor artificiële intelligentie (AI) in de gehele EU. Met dit akkoord van 9 december 2023, dat het Commissievoorstel op verscheidene punten wijzigt, versterkt de EU de wens om te komen tot een mondiale standaard van AI regulering. Dit politieke akkoord heeft nog niet geleid tot een formele wettekst. De Raad en het EP schrijven meer juridisch-technische details van de Verordening uit om tot een gezamenlijke tekst te komen. Voorafgaand aan ondertekening, zal nog een laatste juridisch- en taal-technische controle uitgevoerd worden. De meeste normen zullen twee jaar na de inwerkingtredingsdatum van kracht gaan.

Vooralsnog staat de inwerkingtreding van de AI Verordening gepland in de loop van 2024 (datum nog niet bekend) en heeft vervolgens een periode van twee jaar voor het van kracht worden in alle lidstaten van de EU, omdat deze toegepast/omgezet moeten worden in de nationale wetgeving. Oftewel in 2026 wordt deze AI verordening van kracht. Daarom is het uitzoeken van de impact van deze verordening en de voorbereiding van het implementeren daarvan in de lokale wet- en regelgeving een actiepunt voor de jaren 2024 en 2025, zodat de Gemeente Barneveld daar vóór 2026 op voorbereid is.

Wet open Overheid
Op 1 mei 2022 is de Wet open Overheid (Woo) als opvolger van de Wet openbaarheid van bestuur (Wob) in werking getreden. Het uitgangspunt van de Woo is een actievere openbaarmakingsverplichting en bestaat uit een passieve en een actieve informatieverstrekking. De passieve informatieverstrekking betreft de openbaarmaking van documenten naar aanleiding van een ingediend Woo-verzoek (vergelijkbaar met het Wob-verzoek) is op 1 mei 2022 direct in werking getreden. De actieve openbaarmakingsplicht daarentegen treedt voor verschillende onderdelen gefaseerd in werking. Ook wordt met de Woo 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 van de PO, CISO en FG van belang is. De projectgroep implementatie Woo heeft in de loop van 2023 zowel de juristen als ook de FG aangehaakt bij de projectgroep, zodat alle aspecten van actieve openbaarmaking Woo ook vanuit privacy kritisch bekeken en beoordeeld worden.

Wet Aanpak Meervoudige problematiek Sociaal Domein
De inwerkingtreding van de Wet Aanpak Meervoudige problematiek Sociaal Domein (Wams) stond gepland op 1 januari 2024. Maar uit een nieuwsbericht van de VNG van 22 november 2023 blijkt dat de focus van de handreikingen en checklists niet meer op het wetsvoorstel ligt, maar op het versterken van de aanpak van meervoudige problematiek in het sociaal domein. Dit omdat de wet controversieel is verklaard, maar het wel verstandig is om alvast met het versterken van de aanpak van meervoudige problematiek aan de slag te gaan.

Het is de bedoeling dat in de Wet Wams de wettelijke borging van de regionale meldpunten wordt voorbereid. 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 van de PO, CISO en FG van belang is. Vooralsnog is er nog geen duidelijkheid over de behandeling van dit wetsvoorstel, de datum van inwerkingtreding en de implementatie. Zodra het nieuwe kabinet gevormd is in 2024 zal dit wetsvoorstel weer opgepakt moeten gaan worden. De VNG adviseert gemeenten niet af te wachten, maar al verder te gaan met de nodige voorbereidingen omdat het te verwachten is dat deze wet er wel komt, zij het met enige vertraging.

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.

Vanuit informatieveiligheid blijft aandacht gevraagd worden voor het vergrendelen van het beeldscherm als de werkplek verlaten wordt. 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 of bezoekers, 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 2023 zijn waar nodig protocollen en procedures met betrekking het werken met persoonsgegevens voor afdelingen en/of teams opgesteld en/of geactualiseerd. Nu deze zaken geregeld zijn, is de bescherming van persoonsgegevens beter geborgd. Het is daarbij wel van belang dat deze afspraken nageleefd worden. In 2024 zal een controle op naleving gedaan worden.

Belang: Uit de AVG vloeit voort dat passende technische en organisatorische maatregelen moeten worden genomen ter beveiliging van persoonsgegevens. Een voorbeeld hiervan is logging en controle op de logging (monitoring) bij het gebruik van applicaties. Uit de zelfevaluatie (zie paragraaf 3.5) komt echter naar voren dat logging en monitoring nog niet voor alle applicaties is ingericht. Dat hier eventueel handhavend tegen kan worden opgetreden door de AP, blijkt uit boetes die zijn opgelegd aan andere organisaties, waarbij veelal sprake is van een datalek in combinatie met een gebrekkige logging en monitoring. Bij de uit het Wpg verbeterplan voortkomende zaken is logging en monitoring opnieuw gecontroleerd en beoordeeld. Daardoor zijn er al veel zaken opgepakt en beter geregeld, maar er zijn nog openstaande zaken die verder opgepakt en uitgevoerd moeten worden. Dat komt ook voort uit de uitgevoerde DPIA’s en de daaruit voortgekomen aanbevelingen en te nemen maatregelen.

Aanbeveling: Een volgende stap in het nog beter privacy-proof maken van de gemeente Barneveld is het verder invoeren van passende technische en organisatorische maatregelen, meer specifiek logging en monitoring bij het gebruik van applicaties. Wordt dit niet ingevoerd, dan loopt de gemeente Barneveld op dit vlak een groot risico. Dit is in 2023 opgepakt en zal in 2024 verder uitgevoerd worden.

Belang: Een andere passende technische en organisatorische maatregel ter beveiliging van persoonsgegevens is het op een veilige manier bewaren en verzenden van gegevens. Door het digitale werken kunnen bestanden met persoonsgegevens makkelijker (onbewust) worden bewaard op plekken waar dat niet gewenst is. Hierbij kan gedacht worden aan de persoonlijke e-mailbox in Outlook en Onedrive in plaats van een vak applicatie of het zaaksysteem. Het is van belang dat er binnen de gemeente Barneveld een eenduidige lijn is waar bestanden met persoonsgegevens bewaard moeten worden.

Aanbeveling: In afstemming met stakeholder tot een gedragen werkinstructie te komen waar bestanden met persoonsgegevens moeten worden opgeslagen en op welke wijze deze gedeeld mogen worden met derden. Hierover is in 2023 overleg gevoerd en afstemming gezocht met teamleiders en waar nodig het CT. In meerdere teams is dit al actief opgepakt en 2024 zal in het teken komen te staan van verdere opschoning van schaduwarchieven op onjuiste plaatsen door de onjuiste werkwijze te beëindigen en te zorgen voor opslag in de juiste vak applicaties of het zaaksysteem.

Belang: Uit een DPIA komen maatregelen naar voren die geïmplementeerd moeten worden om mogelijke risico's te mitigeren. De teams dragen zelf verantwoordelijkheid voor het implementeren van de maatregelen. Zonder deze implementatie, blijven risico's bestaan.

Aanbeveling: Er moet structureel een proces komen voor controle op opvolging van de maatregelen uit de DPIA. De FG voert deze controle structureel uit en kan vervolgens toetsen of alle mitigerende maatregelen zijn genomen. In 2023 is er een begin gemaakt met het evalueren van het al dan niet oppakken en uitvoeren van de aanbevelingen en te nemen maatregelen. In 2024 wordt dit verder opgepakt en uitgevoerd, waarbij de FG toezicht houdt op de naleving.

5.2 Acties voor 2024

In de voorgaande hoofdstukken is aangegeven welke werkzaamheden in 2023 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 2024 worden de onderstaande acties opgepakt, waarover in het Jaarverslag FG 2024 gerapporteerd zal worden.

- DPIA’s: evalueren van de opgepakte en uitgevoerde uit de rapportages voortgekomen aanbevelingen en maatregelen. Daarna toezien op de naleving ervan.

- DPIA’s: herzien en actualiseren van uitgevoerde DPIA’s in verband met de 3-jaarlijkse herziening;

- Uitvoering geven aan nog openstaande acties uit het verbeterplan Wpg;

- 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 team- 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. In overleg met het CT is dit niet meer in 2023 opgepakt, maar is dit een actiepunt geworden voor 2024. De teamleiders willen eerst met elkaar en met het CT afstemmen welke periode in het jaar daarvoor het meest geschikt is. Bijvoorbeeld de zomervakantieperiode of de kerstvakantieperiode.

- Actiepunten uit de in januari 2023 gehouden en in januari 2024 te houden zelfevaluatie/borging in 2024 verder oppakken en uitvoeren.

- Uitzoeken impact AI verordening en voorbereiden op implementatie van deze verordening in de lokale wet- en regelgeving in 2024 en 2025, voordat de AI verordening in 2026 van kracht wordt.

- Verbeteren bewustwording privacy en beeld van de privacyregelgeving positiever maken.