ONDERZOEK ALGEMENE VERORDENING GEGEVENS-BESCHERMING

17 februari 2025

REKENKAMER GEMEENTE NEDERWEERT

Inhoudsopgave

Inhoudsopgave

Voorwoord

Na overleg met de leden van de gemeenteraad heeft de rekenkamer van de gemeente Nederweert een aantal potentiële onderzoeksonderwerpen voor 2024 geïdentificeerd. Deze zijn vervolgens gewogen op basis van de criteria opgenomen in het Reglement van Orde van de rekenkamer. Op basis van de uitkomsten van deze weging is besloten in 2024 onder andere onderzoek te doen naar de naleving van de Algemene Verordening Gegevensbescherming (AVG) door de gemeente Nederweert.

Een goede naleving van de AVG door de gemeente is om meerdere redenen van belang. In de eerste plaats omdat gemeenten veel persoonsgegevens, waaronder ook tal van gevoelige (volgens de AVG 'bijzondere') persoonsgegevens, verzamelen en gebruiken om hun taken uit te voeren. Vaak hebben inwoners geen keuze om hun persoonsgegevens wel of niet af te staan, maar zijn ze (wettelijk) verplicht deze aan de gemeente te verstrekken. Burgers en andere belanghebbenden moeten erop kunnen vertrouwen dat gemeenten zorgvuldig met deze gegevens omgaan. Het recht op eerbiediging van de persoonlijke levenssfeer is immers een van de Nederlandse grondrechten.

Gemeenten hebben daarnaast zelf ook belang bij een goede bescherming van de aan hen toevertrouwde persoonsgegevens. Als het mis gaat kan immers forse imagoschade optreden alsmede verlies van vertrouwen in de (gemeentelijke) overheid. Daarnaast bestaat het risico dat forse boetes aan een gemeente worden opgelegd door de Autoriteit Persoonsgegevens indien de gegevensbescherming niet op orde is.

Reden genoeg voor de rekenkamer om na te gaan hoe de gemeente op dit thema ervoor staat. Het onderzoek is uitgevoerd in de periode van mei tot en met december 2024. In dit rapport delen we onze bevindingen daarover.

Tijdens ons onderzoek hebben wij open en prettige gesprekken gevoerd met de portefeuillehouder, het management, talrijke medewerkers van de gemeente Nederweert en enkele partijen die waren ingehuurd voor werkzaamheden op het gebied van gegevensbescherming en toezicht. Afspraken daarvoor werden vlot gemaakt en informatie snel geleverd. Graag spreken wij onze dank uit voor deze uitstekende medewerking.

Rekenkamer Nederweert 18 februari 2025,

Frank Sampers

Clive ter Heege

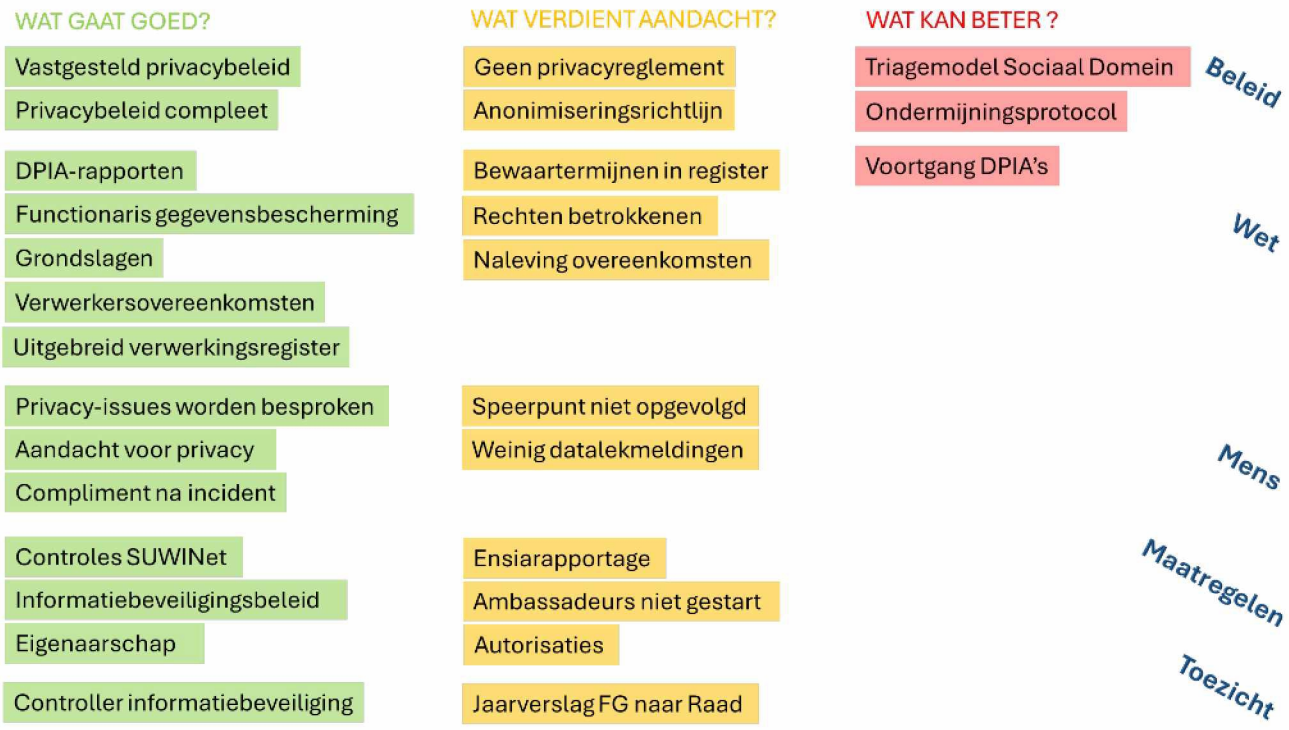
Ayla Hermans

Eric Sentjens

Managementsamenvatting

In dit rapport schetsen we de aanleiding voor het onderzoek, de gevolgde aanpak en de bevindingen. De bevindingen vormen de kern van het rapport

Onderstaand schema toont in één oogopslag de belangrijkste bevindingen. Het is met betrekking tot de verbeterpunten (rood) volledig, bij de andere bevindingen is het schema voor de overzichtelijkheid beperkt tot een selectie. In hoofdstuk 3 staan alle bevindingen vermeld en toegelicht. Een totaaloverzicht van de mogelijke verbeterpunten zonder toelichting treft u aan in bijlage 4.



Bij de bevindingen hebben wij zaken genoemd die naar ons oordeel goed zijn geregeld en de zaken die ruimte bieden voor verbetering. Het onderzoek en de rapportage daarover is in aard kritisch. Dat laat onverlet dat de overallconclusie luidt:

De gemeente Nederweert doet het relatief goed op het gebied van de gegevensbescherming. Een tweetal bij de gemeente actieve onafhankelijke externe adviseurs op het gebied van privacy en AVG, die ook bij andere gemeenten vergelijkbare opdrachten uitvoeren, gaven dit duidelijk aan. Dit neemt niet weg dat het in een aantal gevallen beter kan.

Bij de aanbevelingen naar aanleiding van dit onderzoek maken wij onderscheid in aanbevelingen die zijn gericht aan de gemeenteraad en aanbevelingen die zijn gericht aan het college van burgemeester en wethouders.

De **aanbevelingen aan de gemeenteraad** zijn:

- Vraag het college van burgemeester en wethouders de aan hen gerichte aanbevelingen over te nemen.
- Ga na hoe u uw betrokkenheid bij dit voor de inwoners van de gemeente belangrijke grondrecht kunt versterken. Hierbij adviseren wij tenminste te overwegen of en hoe u zich wilt laten informeren over:
  - het jaarlijkse verslag van de functionaris gegevensbescherming;
  - de daaruit en uit dit rapport voortvloeiende verbeterplannen van het college en de opvolging daarvan;
  - een (beter) integraal beeld van de stand van zaken rondom de informatiebeveiliging in het kader van de ENSIA verantwoording, alsmede de daaruit voortvloeiende verbeterplannen;
  - (ernstige) datalekken .

De **aanbevelingen aan het college van burgemeester en wethouders** zijn:

- Geef het thema gegevensbescherming een nieuwe impuls, gericht op de kwaliteit en kwantiteit van de voor de verantwoordingsplicht vereiste maatregelen en documenten, zoals de DPIA's, alsmede op het verbeteren van de governance, waaronder ook de structurele betrokkenheid van de gemeenteraad bij dit onderwerp.
- Trek het huidige "Privacyprotocol Ondermijning" in en vervang het indien nodig door een versie die voldoet aan de eisen uit de AVG.
- Pas het "Triagemodel voor gegevensdeling bij meervoudig complexe casuïstiek, waarin de wet niet voorziet (sociaal domein)" aan zodat duidelijk is dat binnen de grenzen van de AVG wordt gebleven, geef de privacy officer een adviserende rol in de uitvoering en borg het toezicht op de toepassing van het triagemodel.
- Analyseer de overige bevindingen in dit rapport zoals opgenomen in hoofdstuk 3 en bijlage 4, stel onderbouwd vast of en zo ja welke verbetermaatregelen noodzakelijk of wenselijk zijn en met welke prioriteit. Wijs deze toe aan verantwoordelijken en monitor de voortgang. Informeer in lijn met de eerste aanbeveling de gemeenteraad over de gemaakte keuzes, het verbeterplan en de voortgang daarvan.

1 Inleiding

1.1 Doelstelling

De doelstelling van het onderzoek is als volgt:

> *Inzichtelijk maken aan welke belangrijke onderdelen van de AVG de gemeente Nederweert voldoet en op welke punten er eventueel sprake is van kwetsbaarheden.*

1.2 Leeswijzer

Hoofdstuk 2 beschrijft de onderzoeksopzet en uitvoering. In hoofdstuk 3 geven we onze bevindingen inclusief toelichting weer en in hoofdstuk 4 treft u de conclusies en aanbevelingen aan. In hoofdstuk 5 is de bestuurlijke reactie van het college van burgemeester en wethouders integraal opgenomen. Hoofdstuk 6 betreft het nawoord van de rekenkamer.

2 Onderzoeksopzet en uitvoering

In dit hoofdstuk wordt beschreven hoe het onderzoek is opgezet en uitgevoerd.

2.1 Kernvraag en deelvragen onderzoek

Op basis van de in punt 1.1 opgenomen doelstelling van het onderzoek luidt de kernvraag waarop antwoord wordt gegeven:

Voldoet de gemeente Nederweert aan de belangrijkste vereisten uit de Algemene Verordening Gegevensbescherming?

Om deze vraag te beantwoorden is een vijftal deelonderwerpen onderzocht:

- Het **privacybeleid**.
- De invulling van de belangrijkste **verplichte onderdelen** van de AVG.
- De aandacht voor de **menselijke factor** bij het beschermen van persoonsgegevens.
- De **organisatorische en technische maatregelen** die zijn getroffen om de persoonsgegevens te beveiligen.
- Het **toezicht op** de uitvoering van de verplichte delen van de AVG.

2.2 Normenkader

De normen die tijdens het onderzoek zijn gehanteerd zijn primair gebaseerd op de criteria die zijn opgenomen in het document “Het borgen van de Algemene Verordening Gegevensbescherming in de gemeentelijke organisatie”, ontwikkeld door VNG Realisatie. Deze criteria worden ook gehanteerd door de Functionaris Gegevensbescherming van de gemeente Nederweert in zijn toezichthoudende rol en moeten daarom herkenbaar zijn voor de gemeente Nederweert.

Waar nodig zijn de criteria aangevuld met relevante eisen of dringend suggesties uit andere bronnen, zoals bijvoorbeeld de Autoriteit Persoonsgegevens. Voor de beoordeling van de menselijke factor is het normenkader gebaseerd op de acht cultuurdimensies uit het gedachtegoed over ‘Soft Controls’ van van [redacted] / KPMG.

Het normenkader is samengevat opgenomen in bijlage 1.

2.3 Fasering en aanpak onderzoek

Het onderzoek naar de naleving van de AVG door de gemeente Nederweert heeft plaatsgevonden in een aantal fasen. Het betreft:

- **Vooronderzoek**. In deze fase van het onderzoek heeft binnen het zeer uitgebreide thema van de AVG een nadere afbakening en prioritering plaatsgevonden. Daartoe is een aantal oriënterende gesprekken gevoerd met direct betrokkenen uit de raad, college en gemeentelijke organisatie en is een aantal relevante documenten bestudeerd. Dat heeft geleid tot een voorlopig beeld van welke onderdelen al relatief goed geborgd zijn in de organisatie en daarmee tijdens de onderzoeksfase minder uitgebreid onder de loep genomen worden en

welke onderdelen meer aandacht vragen. Dit leidde tot de conclusie in het onderzoek de focus te leggen op twee deelvragen (de verplichte onderdelen van de AVG en de menselijke factor)

- **Onderzoeksfase**. In de onderzoeksfase is het daadwerkelijke onderzoek uitgevoerd. Daarbij zijn interviews gehouden met betrokken functionarissen en nadere interne en externe stukken onderzocht, opgevraagd en bestudeerd.
- **Analyse en opstellen concept rapport**. In deze fase van het onderzoek is de verkregen informatie geanalyseerd en zijn de uitkomsten daarvan verwerkt in een concept rapport.
- **Ambtelijk wederhoor**. Het concept-rapport is aan de gemeentesecretaris voorgelegd voor ambtelijk wederhoor. De ontvangen reactie is bestudeerd en waar nodig verwerkt in het concept rapport, wat resulteerde in een concept voor bestuurlijk wederhoor.
- **Bestuurlijk** wederhoor. Het concept voor bestuurlijk wederhoor is vervolgens voor bestuurlijk wederhoor aan het college aangeboden. De bestuurlijke reactie is opgenomen in hoofdstuk 5 van dit rapport.
- **Definitieve rapportage**. Het definitieve rapport inclusief het nawoord van de rekenkamer, opgenomen in hoofdstuk 6, is tenslotte aangeboden aan de gemeenteraad van Nederweert en openbaar gemaakt.

De lijst van door ons geïnterviewde functionarissen treft u aan in bijlage 2. Het overzicht van door ons geraadpleegde stukken is opgenomen in bijlage 3. Een totaaloverzicht van alle mogelijke verbeterpunten zonder toelichting treft u aan in bijlage 4.

3 Bevindingen

3.1 Inleiding

In dit hoofdstuk treft u onze belangrijkste bevindingen aan. Deze worden per deelvraag (zie paragraaf 2.1) gepresenteerd.

Bij de bevindingen hebben wij naast de zaken die ruimte bieden voor verbetering zoveel als mogelijk ook de zaken genoemd die naar ons oordeel goed geregeld zijn. Mocht het gevoel ontstaan dat de negatieve bevindingen de overhand hebben, dan roepen wij graag de eerste alinea van de managementsamenvatting in herinnering: de gemeente Nederweert doet het relatief goed op het gebied van de gegevensbescherming, maar het kan in een aantal gevallen beter.

3.2 Het privacybeleid

3.2.1 Inleiding

Algemeen

Het privacybeleid van de gemeente Nederweert geeft richting aan en kaders voor de uitvoering van de gegevensbescherming en het toezicht daarop door de gemeente. Het is daarmee zowel formeel (juridisch) als praktisch de basis voor de uitvoering en het toezicht. Wij hebben onderzocht of het beleid toereikend is om deze belangrijke functies waar te kunnen maken.

Het privacybeleid van de gemeente Nederweert is vastgelegd in een tweetal documenten:

- Het Privacybeleid gemeente Nederweert 2020 – 2023. Dit document wordt aangeduid als het ‘interne privacybeleid’. Gedurende de laatste weken van het onderzoek is binnen de gemeente gewerkt aan een concept van een nieuw beleidsstuk voor 2024-2025. Onlangs is dat in het managementteam (MT) geaccordeerd, maar ten tijde van het schrijven van het rapport nog niet door het college vastgesteld. Wij hebben een concept van het beoogde nieuwe beleid in mogen zien en hebben onze bevindingen daarover meegenomen in dit rapport in de hoop dat deze meegewogen kunnen worden voordat het nieuwe beleid wordt vastgesteld. Het grootste deel van de bevindingen betreffen echter het nu nog geldende ‘oude’ beleid
- Het Privacybeleid gemeente Nederweert. Dit document wordt benoemd als ‘extern privacybeleid’.

In een online beschikbare Privacyverklaring wordt een aantal onderwerpen uit het privacybeleid nader toegelicht. Daarnaast is het privacybeleid onlosmakelijk verbonden met het informatiebeveiligingsbeleid van de gemeente Nederweert.

Diepgang en scope onderzoek privacybeleid

Tijdens de oriënterende fase van het onderzoek is bij de rekenkamer het beeld ontstaan dat het privacybeleid van de gemeente Nederweert geen diepgaand onderzoek behoefde. Gezien het belang van goed beleid als fundament voor de overige facetten van de gegevensbescherming, hebben we echter wel besloten een aantal relevante kenmerken van het privacybeleid kritisch te bezien. De

uitkomsten daarvan treft u hierna aan. Bij de uitvoering van het onderzoek vormde het beleid tevens een norm, waarmee de uitvoering ervan op een aantal vlakken is beoordeeld.

3.2.2 Bevindingen ten aanzien van het privacybeleid

Delen van het 'interne' privacybeleid zijn strijdig met de AVG

Het staat buiten kijf dat een overheidsorganisatie als de gemeente Nederweert gebonden is aan de geldende wet- en regelgeving. Het privacybeleid van de gemeente Nederweert dient er dan ook ondubbelzinnig op gericht te zijn dat de gemeentelijke taken worden uitgevoerd binnen de kaders van de privacywetgeving. Op talrijke plaatsen in het privacybeleid treffen wij teksten aan die dit uitgangspunt bekrachtigen.

Wij constateren echter ook dat een aantal onderdelen van het 'interne' privacybeleid meer ambigu zijn en tenminste lijken te suggereren dat door gemeentefunctionarissen kan worden besloten de privacywetgeving ondergeschikt te maken aan andere belangen. Zo wordt in hoofdstuk 3, met de veelzeggende titel "Privacy is vooral een belangenafweging", de vraag gesteld wie binnen de organisatie beslist of het belang van de privacy en de daarvoor te treffen maatregelen opwegen tegen 'het organisatiebelang' en wordt het beantwoorden van die vraag aangemerkt als onderdeel van het privacybeleid. Deze opmerking suggereert dat iemand in de gemeentelijke organisatie de bevoegdheid heeft om het belang van (het grond)recht op privacy en de wettelijk vastgelegde bepalingen daarover af te wegen tegen 'het organisatiebelang' van de gemeente.

verderop op dezelfde bladzijde wordt onder punt 3 van de kop "2. Beleid ten aanzien van gebruik van persoonsgegevens algemeen" terecht gesteld dat het delen van gegevens is gebaseerd op de mogelijkheden die de wet biedt. De zin gaat echter verder met de opmerking dat in die gevallen waarin de wet niet voorziet (dus waar geen wettelijk kader aanwezig is), een 'noodzakelijkheidstoets' wordt uitgevoerd, waarbij wordt verwezen naar het triagemodel in bijlage 3 van het document. Dit betekent dat indien iemand in de gemeente het als 'noodzakelijk' bestempelt deze functionaris, ook zonder wettelijk kader, persoonsgegevens zou mogen delen. Deze functionaris is volgens het opgestelde model niet verplicht zijn (voorgenomen) besluit hiertoe af te stemmen met de Privacy Officer.

In punt 6 van hoofdstuk 4 van het 'interne' privacybeleid wordt onder de kop '6.1.a Overleg over cliënten' benadrukt dat de wetgever omwille van de privacybescherming geen regels heeft gegeven die het delen van gegevens in het sociale domein vereenvoudigt. Ook wordt gesteld dat daardoor in het geval van de WMO 2015 dat de WMO-consulent toestemming van de betrokkene nodig heeft om de reeds bij de gemeente beschikbare gegevens over een uitkering of schuld op te vragen bij de bijstandsconsulent respectievelijk de medewerker schuldhulpverlening. Des te opvallender is het dat in punt 3 van het triagemodel wordt gesteld dat de interne of externe professional/hulpverlener ook zonder wettelijke basis of toestemming van betrokkene kan bepalen toch tot het delen van (bijzondere) persoonsgegevens over te gaan indien deze van mening is dat dit voor de dienstverlening zeer dringend noodzakelijk is. In gesprekken hierover werd aangegeven dat het dan moet gaan om 'schrijnende gevallen', maar een heldere aanduiding van wat wel en niet als 'schrijnend' moet worden beschouwd, is niet vastgelegd en kon niet worden gegeven.

Ten aanzien van het thema voorkomen en bestrijden van ondermijnende criminaliteit is eveneens sprake van strijdigheid met de AVG. Dat wordt in het betreffende beleid ook als zodanig verwoord.

In het 'Privacyprotocol Ondermijning'[1] wordt opgemerkt dat een belangrijk deel van de informatie waarover de gemeente beschikt in het kader van het uitvoeren van haar taken gebonden is aan privacywetgeving waardoor het delen van gegevens niet is toegestaan of aan zware beperkingen is gebonden. Gesteld wordt dat de ruimte voor gegevensuitwisseling vanuit sommige taakvelden zeer beperkt is of ontbreekt, maar dat de noodzaak tot gegevensuitwisseling soms zeer urgent is en er in dat soort gevallen toch de behoefte is om over te gaan tot het delen van informatie. Ook hier wordt een dilemma geschetst, waarbij het afwegen van de tegengestelde belangen nodig is alsmede besluitvorming daarover. Het protocol moet bestuur en management een kader te bieden daarvoor alsmede om de benodigde waarborgen in bouwen die eventuele risico's voor de privacybescherming tot een minimum beperken.

In de toelichting bij het protocol wordt nadrukkelijk vermeld dat het niet is toegestaan informatie die is verzameld voor andere doeleinden te gebruiken voor het voorkomen en bestrijden van ondermijnende criminaliteit: "*... heeft de wetgever het gemeentebestuur niet voorzien van een wettelijke grondslag voor dit handelen. Dat maakt het lastig om voor de verwerking van persoonsgegevens een grondslag te vinden in de Algemene verordening gegevensbescherming (AVG). Als geen grondslag kan worden aangewezen, is er vanuit privacy oogpunt geen basis voor het verwerken van persoonsgegevens door de gemeente voor onderzoek naar activiteiten van ondermijning en georganiseerde criminaliteit. De aanpak van ondermijning houdt namelijk in het verwerken van persoonsgegevens voor een ander doel dan waarvoor deze gegevens oorspronkelijk zijn verzameld. Informatie wordt verzameld vanuit verschillende taken en bevoegdheden, om het vervolgens voor een nieuw doel te gebruiken. Dat nieuwe doel, vaststellen van ondermijning, is nog niet wettelijk vastgelegd. Dit is het grootste knelpunt.*"

Dat is volkomen juist. Er wordt echter iets verderop gesteld: "*We kunnen niet wachten op wetgeving. Er is wetgeving in de maak voor het delen van gegevens in samenwerkingsverbanden. De vraag is of deze wet het dilemma gaat oplossen en toepasbaar is binnen een gemeente en wanneer deze van kracht wordt. Daarnaast is er een advies van de Raad van State, die stelt dat er al veel mogelijk is als het gaat om het delen van gegevens in het kader van de aanpak van georganiseerde misdaad. De uitwerking van die mogelijkheden laat vervolgens op zich wachten. De georganiseerde criminaliteit wacht daar niet op en de gemeente kan het zich niet permitteren om stil te zitten. Daarom is het noodzakelijk om vooruitlopend op toekomstige regels, voor de gemeente Nederweert een protocol op te stellen voor het delen van informatie in die situaties dat de wetgever er niet in heeft voorzien*"

Dat de gemeente ervaart dat de beperkingen die de privacywetgeving oplegt in een aantal gevallen haar belemmert in de taakuitoefening, of deze zelfs vrijwel onmogelijk maakt, is duidelijk en begrijpelijk. Dat het als frustrerend wordt beleefd en dat er, vanuit het ervaren belang van de betreffende taken, getracht wordt daar iets aan te doen is dat ook. Bovendien siert het de gemeente Nederweert dat zij bij de uitwerking van deze materie duidelijk veel moeite heeft gedaan om het verwerken van persoonsgegevens in deze situaties zo zorgvuldig mogelijk plaats te laten vinden. Er is veel tijd en inspanning gestoken in het ontwikkelen van het triagemodel en het privacyprotocol ondermijning, waarmee op gedegen en zorgvuldige wijze de negatieve gevolgen voor de privacy aantoonbaar tot een minimum worden beperkt. Dat laat echter onverlet dat de beschreven werkwijzen naar onze mening strijdig zijn met de privacywetgeving en daarmee onrechtmatig zijn.

[1]Formeel bekend als 'Besluit van het college van burgemeester en wethouders van de gemeente Nederweert houdende regels omtrent privacy (Privacyprotocol Ondermijning Nederweert 2020)'.

In het recent verschenen 'Sectorbeeld Overheid' gaat de Autoriteit Persoonsgegevens in op deze problematiek en is hij volstrekt helder: "*Gemeenten delen en koppelen gegevens vaak vanuit goede intenties, zoals iemand met een zorgvraag helpen, schuldenproblematiek tegengaan of criminaliteit een halt toeroepen. Dit neemt niet weg dat hiervoor een juridische grondslag nodig is. Zonder grondslag mogen organisaties persoonsgegevens niet verwerken, ongeacht eventuele getroffen maatregelen of opgestelde handreikingen.*"

De Autoriteit Persoonsgegevens laat in genoemd document ook geen twijfel bestaan over de vraag of hij dit zal accepteren: "*De AP zal hard ingrijpen bij gemeenten die bij de bestrijding van criminaliteit in het fysieke domein de privacybelangen van burgers in het digitale domein onrechtmatig schenden. Gemeenten hebben niet alleen als taak de openbare orde in de fysieke ruimte te handhaven, maar dienen ook de belangen van burgers in de digitale ruimte te respecteren.*"

Deze uitlatingen van de Autoriteit Persoonsgegevens, versterken onze opvatting dat de gemeente Nederweert zich met het genoemde beleid op zeer glad ijs bevindt.

Overigens is tijdens een interview aan ons te kennen gegeven dat bewust geen gebruik wordt gemaakt van de omstreden mogelijkheden die het privacyprotocol ondermijning biedt, mede omdat op uitvoeringsniveau getwijfeld wordt aan de rechtmatigheid ervan.

De inhoud van het beleid dekt de meeste belangrijke aspecten van de AVG af

De privacybeleidsstukken omvatten gezamenlijk vrijwel alle voor de gemeente essentiële onderdelen van de AVG. In de privacyverklaring wordt bovendien een aantal elementen daarvan verder uitgewerkt. Wat wij onvoldoende in het beleid hebben kunnen terugvinden is beleidsmatige informatie over het (verplichte) datalekregister.

Het privacybeleid is formeel vastgesteld

Beide privacybeleidsstukken zijn in de vergadering van het College van Burgemeester en Wethouders van 17 maart 2020 formeel vastgesteld.

Van het 'externe' privacybeleid staat ook de oude versie nog als geldig online

In het formeel op Overheid.nl gepubliceerde versie van het 'externe' Privacybeleid gemeente Nederweert staat direct voor de ondertekening dat met de inwerkingtreding van dit beleid de Privacyverordening gemeente [redacted] wordt ingetrokken. Dat beleid staat echter nog steeds als 'geldend' op Overheid.nl (https://lokaleregelgeving.overheid.nl/CVDR216190), wat verwarring kan veroorzaken.

Het 'interne' privacybeleid is verlopen en staat als conceptversie in JOIN. Aan vervanging wordt gewerkt, maar roept vragen op

Het 'interne' privacybeleid gemeente Nederweert 2020 – 2023 is inmiddels bijna een jaar verlopen. Alle betrokkenen zijn zich hiervan bewust en geven aan dat er aan een nieuwe versie wordt gewerkt. Ook blijkt vier jaar lang enkel de conceptversie binnen de organisatie gepubliceerd te zijn geweest.

Tijdens het onderzoek hebben wij uitleg gekregen over de gedachten achter het nieuw op te stellen privacybeleid (vereenvoudigen) en hebben we een conceptversie (v.0.9) mogen lezen. Ofschoon het (nog) geen formeel vastgesteld document is, willen we toch opmerken dat het beleid in deze vorm

onvoldoende aansluit op de “tip” van de AP dat een professioneel privacybeleid een concrete vertaalslag van de AVG-normen naar de gegevensverwerkingen van de gemeente moet vormen en dat normen uit de AVG herhalen niet voldoende is. In de versie die wij hebben gelezen worden diverse relevante termen en uitgangspunten uit de AVG nader uitgelegd, wat voor de gebruikers van het beleid verhelderend kan werken. Met uitzondering van de bijlage opgenomen taken en verantwoordelijkheden, gaat het document echter niet of nauwelijks in op wat dit vervolgens concreet voor de gemeente Nederweert inhoudt en hoe daaraan concreet invulling wordt gegeven. Het beoogde nieuwe beleid beperkt zich op deze wijze in hoge mate tot het herhalen van de (in algemene termen nader uitgelegde) normen uit de AVG. Bovendien is een aantal in het eerder vastgestelde beleid opgenomen uitwerkingen daarmee verdwenen uit het privacybeleid, terwijl er geen andere vastlegging van deze benodigde uitwerkingen voor in de plaats is gekomen. De opsteller van het nieuwe conceptbeleid bevestigt dit, omschrijft de ‘verdwenen’ uitwerkingen als werkinstructies en geeft aan dat ze kunnen landen. Over waar dat dan zou zijn, was nog geen besluit genomen.

Het privacybeleid is versnipperd en niet volledig openbaar gemaakt

Ofschoon zoals hiervoor vermeld de beide privacybeleidsstukken vrijwel alle voor de gemeente essentiële onderdelen van de AVG afdekken, merken wij op dat deze informatie versnipperd over beide documenten terug te vinden is. Enkel in onderlinge samenhang is de informatie terug te vinden. Bovendien blijkt het ‘interne’ privacybeleid niet openbaar te zijn gemaakt, waardoor het integrale beeld voor de burger niet beschikbaar is.

De gemeenteraad is slechts beperkt betrokken geweest bij het privacybeleid

De gemeenteraad is met een raadsinformatievoorziening[2] op de hoogte gebracht van het feit dat het beleid is vastgesteld en beknopt geïnformeerd over zijn rol en betrokkenheid ten aanzien van de eigen gegevensbescherming. Het interne privacybeleid is niet bij de raadsinformatievoorziening gevoegd. Wel wordt aangegeven dat het college indien gewenst, op verzoek van de raad, het interne privacybeleid aan de raad zal toesturen. Voor zover wij weten heeft de raad daartoe geen verzoek ingediend. Het veel kortere externe privacybeleid was wel bij de raadsinformatievoorziening gevoegd.

Het privacyreglement voor persoonsgegevens van personeelsleden bestaat niet

In hoofdstuk 4, punt 1.2 van het interne privacybeleid is vermeld dat de verwerking van persoonsgegevens van personeelsleden is vastgelegd in een privacyreglement en dat het privacyreglement jaarlijks wordt geactualiseerd. Ondanks brede navraag binnen de gemeente, bleek niemand dit reglement te kennen. Wij gaan er dan ook vanuit dat het niet bestaat.

Er is een regeling protocol internetgebruik en e-mail

Een deel van de privacy van de medewerkers wordt geregeld in de regeling protocol internetgebruik en e-mail dat onder hoofdstuk 16 van het personeelshandboek is opgenomen. Het protocol bevat afspraken over de wijze waarop de gemeente als werkgever omgaat met het registeren, verzamelen en monitoren van tot een persoon herleidbare data omtrent e-mail- en internetgebruik. Met als doel een goede balans te vinden tussen een verantwoord gebruik van internet en e-mail en bescherming van de privacy van werknemers op de werkplek.

[2]RIV-20-00408 d.d. 24 februari 2020

De anonimiseringsrichtlijn beschermt de privacy van medewerkers niet

Uit punt 1.b van de anonimiseringsrichtlijn Nederweert 2024 maken wij op dat namen van ambtenaren die als opsteller, behandelaar etc. genoemd worden in stukken van de gemeente in principe blijven staan op het document bij openbaarmaking. Daarmee wordt de privacy van de medewerkers van de gemeente niet gewaarborgd. Navraag bij de Functionaris Gegevensbescherming (FG) heeft geleerd dat het niet de intentie was dat het zo in de richtlijn staat. Het juiste uitgangspunt is dat namen van mensen met een publieke functie (wethouder, burgemeester, e.d.) niet geanonimiseerd hoeven te worden, maar van medewerkers met een minder publieke functie wel.

In de praktijk zien wij ook tal van openbaar gemaakte gemeentelijke documenten waarop – in lijn met het onjuist geformuleerde beleid – de namen van met name de opstellers/behandelaars niet zijn geanonimiseerd.

De Ondernemingsraad (OR) is niet betrokken bij het privacybeleid en de uitvoering

De OR heeft ingestemd met het Personeelshandboek Gemeente Nederweert 2023 en daarmee ook met de onderdelen daarin die een relatie hebben met de gegevensbescherming. Tijdens het interview dat wij hadden met de voorzitter van de OR bleek echter geen betrokkenheid te bestaan met het privacybeleid als zodanig en de uitvoering daarvan. Er is vanuit de OR beperkt kennis over hoe er in de organisatie wordt omgegaan met de privacyregels.

Overigens wordt de OR ook niet van de kant van de medewerkers betrokken bij privacygerelateerde zaken; de OR krijgt geen vragen of klachten op dat gebied.

3.3 De verplichte onderdelen van de AVG

3.3.1 Inleiding

Algemeen

De AVG kent tal van regels waaraan een organisatie verplicht dient te voldoen als deze persoonsgegevens verwerkt. De AVG kent bovendien een verantwoordingsplicht. Die houdt onder andere in dat de organisatie moet kunnen aantonen dat wordt voldaan aan de belangrijkste uitgangspunten van de AVG. Wanneer de Autoriteit Persoonsgegevens daarnaar vraagt, is het verplicht hierover verantwoording af te leggen.

Diepgang en scope onderzoek verplichte onderdelen AVG

De onderdelen van de AVG die in de verantwoordingsplicht zijn opgenomen, zijn niet alleen van belang om in formele zin na een verzoek van de AP aan te kunnen tonen dat aan de AVG regels wordt voldaan, maar dragen ook bij aan de richting, sturing en beheersing van de gegevensbescherming.

Gelet op dit dubbele belang van de verplichte onderdelen van de AVG, hebben wij dit onderdeel met meer diepgang in beschouwing genomen. De scope bestaat uit de verplichte onderdelen en de eisen die daaraan worden gesteld, alsmede elementen uit het ‘borgingsproduct’ van de VNG “Het borgen van de Algemene Verordening Gegevensbescherming in de gemeentelijke organisatie” die daaraan bijdragen. Het betreft:

- Verwerkingsregister(s)
- Functionaris voor de gegevensbescherming.
- Privacyverklaring
- Data Protection Impact Assessments
- Verwerkersovereenkomsten
- Datalekregister
- Procedures datalekken
- Toestemming van betrokkenen
- Procedures voor afhandelen verzoeken van rechten betrokkenen
- De eisen gesteld aan geautomatiseerde beslissingen
- Borging gegevensbescherming in samenwerkingsverbanden

In de volgende paragraaf zijn onze bevindingen beschreven.

3.3.2 Bevindingen ten aanzien van de verplichte onderdelen van de AVG

3.3.2.1 Het verwerkingsregister

Er is een verwerkingsregister die qua verwerkingen volledig lijkt

De gemeente Nederweert beschikt over een verwerkingsregister waarin op het moment van het onderzoek 130 verwerkingen waren opgenomen. Het is niet mogelijk de volledigheid van het register vast te stellen, maar duidelijk is dat in het recente verleden gemeentebreed een significante inspanning is geleverd om zo veel mogelijk verwerkingen in kaart te brengen.
De wet schrijft voor welke informatie het register moet bevatten voor elke in het verwerkingsregister opgenomen verwerking. De gehanteerde indeling van het register biedt de mogelijkheid alle verplichte informatie op te nemen.

Er is tenminste één verantwoordelijke voor het onderhoud en beheer van het register

In het privacybeleid (o.a. pt 3.4) is centraal beheer van het register verwerkingsactiviteiten en het verwerken van wijzigingen vanuit de organisatie bij privacy officer belegd. Dit is in de praktijk ook het geval gebleken.

Het verwerkingsregister wordt jaarlijks geactualiseerd en opnieuw vastgesteld door het college en ter kennisname aan de gemeenteraad aangeboden

Het verwerkingsregister wordt jaarlijks door de privacy officer geactualiseerd op basis van input van de diverse onderdelen van de gemeente. De geactualiseerde versie wordt door het college vastgesteld en met een Raadinformatiebrief aan de raad aangeboden. Het verwerkingsregister 2024 is op 7 mei 2024 door het college goedgekeurd en op 8 mei 2024 is de openbare versie met Raadinformatiebrief nr. RIV-24-00851 ter kennisname aan de raad aangeboden.

De juistheid, volledigheid en relevantie van de bij de verwerkingen opgenomen informatie is wisselend

De doeleinden van de verwerkingen en de betrokkenen van wie de persoonsgegevens worden verwerkt zijn over het algemeen goed vastgelegd. Andere onderdelen van het register, in het bijzonder de bewaartermijnen, verdienen aandacht.
Ook de wijze waarop de gemeente haar verantwoordelijkheid voor de naleving van de AVG vorm geeft in situaties waarin sprake is van gezamenlijke verantwoordelijkheid met andere organisaties ontbreekt vrijwel geheel in het verwerkingsregister.

'Overkoepelende/administratieve' informatie ontbreekt bij het verwerkingsregister

Een aantal 'overkoepelende/administratieve' gegevens die volgens de AVG opgenomen dienen te zijn in/bij het verwerkingsregister ontbreekt. Het betreft:

- de naam en contactgegevens van de eigen organisatie
- de naam en contactgegevens van andere organisaties met wie de gemeente gezamenlijk de doelen van en middelen voor de verwerking heeft vastgesteld (gezamenlijke verantwoordelijkheid)
- de functionaris gegevensbescherming
- een algemene beschrijving van de technische en organisatorische maatregelen die zijn genomen om de persoonsgegevens te beveiligen.

Proceseigenaren weten aan wie zij wijzigingen van de bestaande verwerkingen of het toevoegen van nieuwe verwerkingen kunnen doorgeven.

De teamleiders die wij hebben gesproken zijn bekend met het wijzigingsproces en aan wie wijzigingen doorgegeven dienen te worden.

3.3.2.2 De Functionaris Gegevensbescherming

Er is een functionaris gegevensbescherming

De gemeente Nederweert maakt gebruik van een extern ingehuurde FG. Deze is 16 – 18 dagen per jaar voor de gemeente beschikbaar. Tijdens de gesprekken met de rekenkamer maakt de FG een deskundige indruk en geeft er blijk van de organisatie en werkwijze van de gemeente goed te kennen. Ook lijkt hij goed op de hoogte van wat er speelt op het gebied van gegevensbescherming bij de gemeente Nederweert. Hij heeft desgewenst zonder belemmering toegang tot de Gemeentesecretaris.

Het is niet voor iedereen in de organisatie duidelijk wie de FG is en wat zijn taken zijn

Hoewel de FG en zijn taken bij de meest direct bij de AVG betrokken actoren in de gemeente zeker bekend zijn, is bij anderen het beeld wisselend. Het blijkt niet voor iedereen duidelijk hoe de taken van PO/CISO en FG precies zijn afgebakend. Soms is ook niet bekend wie de FG precies is, maar dat is, indien nodig, snel te achterhalen. De FG wordt regelmatig als adviseur ingeschakeld bij privacy-vraagstukken.
Opmerkelijk is dat in art 16 lid 4 van de (nieuwe) organisatieregeling Nederweert 2024 de scope van de rapportage van de FG beperkt lijkt te worden tot informatiebeveiliging, informatiebeveiligingsincidenten en de afhandeling daarvan, terwijl diens verantwoordelijkheden anders en veel breder zijn.

Aan de overige eisen ten aanzien van de FG wordt voldaan.

De gemeente en de FG voldoen aan de overige eisen die de AVG aan deze functie stelt inzake betrokkenheid, autonomie, bereikbaarheid, (on)gevraagd advies, deskundigheid en advisering bij DPIA's.

3.3.2.3 De Privacyverklaring

Er is een privacyverklaring opgesteld en op het internet beschikbaar gesteld

Zoals reeds vermeld onder punt 3.2.1 heeft de gemeente Nederweert een privacyverklaring opgesteld en op de gemeentelijke website gepubliceerd.

De privacyverklaring voldoet aan de meeste, maar niet aan alle daarvoor geldende eisen

De AVG stelt een aantal specifieke eisen aan een privacyverklaring. Deze eisen gaan over de inhoud, de toegankelijkheid en de duidelijkheid van de informatie. De privacyverklaring van de gemeente Nederweert voldoet aan de meeste eisen die de AVG stelt.
De privacyverklaring lijkt met de openingsregel enkel en alleen gericht aan bezoekers van de website: "De gemeente Nederweert respecteert uw privacy als bezoeker van onze website". De verklaring zal zich echter tot een breder publiek (alle burgers en partners van de gemeente) moeten richten.
Aan de eis om te vermelden dat de betrokkenen het recht om de toestemming die zij voor een bepaalde verwerking hebben gegeven, altijd weer mogen intrekken, wordt niet voldaan.

Ook aan de eisen:

- om aan te geven of de betrokkenen verplicht zijn de persoonsgegevens te verstrekken en zo ja, waarom en wat de gevolgen zijn als zij de gegevens niet verstrekken;
- of gebruik wordt gemaakt van geautomatiseerde besluitvorming, inclusief profilering. En zo ja, hoe die besluiten worden genomen;
- als de gegevens van een andere organisatie zijn verkregen: de bron waar de persoonsgegevens vandaan komen. En of de gegevens afkomstig zijn van openbare bronnen;
- of de gemeente van plan is de persoonsgegevens door te geven buiten de EU of aan een internationale organisatie. En zo ja, op welke juridische grond dit wordt gedaan

wordt niet voldaan.

Tenslotte is in de privacyverklaring de tekst over de doeleinden zodanig geformuleerd ("Als u gebruik maakt van diensten of producten van de gemeente hebben wij persoonsgegevens van u nodig") dat een betrokkene eruit zou kunnen lezen dat alleen persoonsgegevens worden verwerkt als hij/zij actief ervoor kiest gebruik te maken van producten of diensten van de gemeente. Dat is uiteraard in de meeste gevallen niet de situatie.

3.3.2.4 De Data Protection Impact Assessments (DPIA's)

Het verwerkingsregister maakt niet inzichtelijk welke bestaande verwerkingen een hoog privacyrisico opleveren, noch hebben wij elders een dergelijk overzicht gevonden

Het verwerkingsregister kent een veld 'Bijzonderheden, bijvoorbeeld DPIA', waar per verwerking kan worden vermeld of een DPIA is uitgevoerd dan wel nog moet worden uitgevoerd. Op enkele uitzonderingen na is dat veld echter niet ingevuld. Hoge privacyrisico's worden evenmin benoemd in het register.

Het aantal uitgevoerde DPIA's blijft achter bij wat mag worden verwacht

Veel verwerkingen waarvoor DPIA's mogen worden verwacht op basis van de lijst met hoog risicoprocessen van de informatiebeveiligingsdienst van de VNG, zijn niet benoemd in het verwerkingsregister en zijn voor zover wij hebben kunnen vaststellen ook niet uitgevoerd noch gepland. Dit sluit aan bij de bevinding in het meest recente jaarverslag (2023-2024) van de FG die voor het tweede jaar op rij vaststelt dat de DPIA's achterlopen. Dit betreft zowel de beoordeling of een DPIA aan de orde is, de planning als de uitvoering van de DPIA.

De DPIA's die we hebben gezien voldoen aan de eisen

We hebben een aantal rapportages van uitgevoerde DPIA's ontvangen en bestudeerd. De rapporten zien volledig en zorgvuldig opgesteld uit en vermelden in hoeverre bevindingen uit de uitgevoerde analyse zijn opgevolgd.

De verantwoordelijkheden rondom DPIA's zijn beschreven in het beleid, maar worden in de praktijk niet altijd ingevuld

Volgens hoofdstuk 4, punt 2 van het interne privacybeleid is het MT opdrachtgever voor DPIA's en beslist over de aanpak van een DPIA. De privacy officer adviseert het management en de organisatie over de uitvoering van en de opvolging van aanbevelingen naar aanleiding van een DPIA. In praktijk zien we dit echter niet terug. Binnen het MT lijkt het structurele zicht op deze rol en op dit proces niet bij iedereen aanwezig. Volgens de privacy officer is er ook nog geen bewaking (voortgang, opvolging bevindingen) met betrekking tot DPIA's geformaliseerd. Met de introductie van het nieuwe Informatiebeveiligings Management Systeem (IBMS, 'Recourse') verwacht de privacy officer dat dit gaat verbeteren.

In het interne privacybeleid staat verder dat de externe privacydeskundige (adviseur) onder andere de taak heeft DPIA's uit te voeren. Desgevraagd gaf betrokkene tijdens ons interview niet bekend te zijn met deze passage.

3.3.2.5 De verwerkersovereenkomsten

De gemeente heeft een overzicht van verwerkers die in hun opdracht persoonsgegevens verwerken; deze is echter niet in alle gevallen actueel

De verwerkers van persoonsgegevens door derden in opdracht van de gemeente zijn terug te vinden in het verwerkingsregister. De volledigheid hebben wij niet kunnen vaststellen, maar de meeste verwerkers lijken te zijn opgenomen. De actualiteit van de informatie laat ruimte voor verbetering.

Door ons bekeken verwerkersovereenkomsten bevatten alle vereiste onderdelen

Wij hebben een beperkt aantal verwerkersovereenkomsten uit het sociale domein inhoudelijk bekeken en geconstateerd dat alle vereiste onderdelen daarin waren opgenomen en uitgewerkt en dat de overeenkomsten door daartoe bevoegde functionarissen bij de gemeente en de verwerker zijn ondertekend. De onderzochte overeenkomsten kennen geen uniforme opmaak en zijn (daarmee) niet allemaal in lijn met het VNG-model.

Er is weinig structureel toezicht op de gemaakte afspraken

In de overeenkomsten afspraken staan over het toelaten van audits door of namens de opdrachtgever. In de praktijk blijkt echter weinig tot geen toezicht plaats te vinden op de naleving van de in de verwerkersovereenkomsten gemaakte afspraken, zoals bijvoorbeeld de bewaartermijnen en de IT beveiliging. Daarbij is voor zover wij hebben kunnen nagaan ook geen onderscheid gemaakt op basis van de aard van de verwerkte persoonsgegevens of uitkomsten van risicoanalyses. Tijdens de gehouden interviews werd vooral gesproken in termen als ‘vertrouwen’, ‘alleen als er aanleiding voor is en dat is tot nu toe niet het geval geweest’, ‘dat is ondoenlijk’ etc.

3.3.2.6 Het datalekregister

Er is een datalekregister aanwezig, echter niet alles wordt daarin vastgelegd

Het verplichte datalekregister is aanwezig en aan ons getoond. Ons is gezegd dat sinds de aansluiting op het centrale incidenten proces van ICT NM (sinds 1 juni 2024) bij het besluit om een onregelmatigheid in het register op te nemen onderscheid wordt gemaakt tussen ‘gebeurtenissen’ en ‘incidenten’. Een gebeurtenis wordt daarbij gedefinieerd als een onregelmatigheid waarbij zich enkel een risico op een inbreuk voordoet, maar waarbij geen feitelijke inbreuk optreedt. Als voorbeeld werd daarbij genoemd dat iemand wegloopt van de werkplek zonder het scherm van zijn of haar computer te vergrendelen. Dit is een gebeurtenis. Pas als iemand vervolgens gebruik maakt van deze situatie door kennis te nemen van informatie die via de betreffende computer beschikbaar is, wordt het een incident. Alleen incidenten worden geregistreerd in het datalekregister, gebeurtenissen niet. Volgens de CISO is dat mogelijk door het geringe aantal ambtenaren bij de gemeente Nederweert, waardoor hij weet waar als gevolg van de gebeurtenissen extra aandacht nodig is.

Het genoemde onderscheid komt niet overeen met de terminologie in het document van VNG Realisatie (Het borgen van de Algemene Verordening Gegevensbescherming in de gemeentelijke organisatie), waar wordt geschreven over ‘inbreuken en incidenten’. Dat wekt verwarring op. Het niet registreren van ‘gebeurtenissen’ omdat de CISO deze kennis kan onthouden, is risicovol omdat bij langere afwezigheid of vertrek van de CISO het risico bestaat dat deze informatie niet (meer) beschikbaar is. Bovendien worden deze gebeurtenissen hierdoor niet gedeeld met leidinggevenden en teams, waardoor ze niet bijdragen aan preventie en bewustzijn.

De vereiste inhoudelijke gegevens per datalek zijn aanwezig in het datalekregister

In het datalekregister zijn per datalek gegevens opgenomen over de feiten ervan (wat is er gebeurd en welke persoonsgegevens betreft het), de gevolgen van het lek en de genomen correctieve maatregelen.

Delen van de benodigde procesmatige informatie ontbreekt in het datalekregister

Ofschoon in het datalekregister wel wordt vermeld of de FG bij de afdoening is betrokken, wordt niet aangegeven welke adviezen de FG heeft gegeven. In sommige gevallen wordt wel (summier) vermeld waarom de Autoriteit Persoonsgegevens niet is geïnformeerd, maar in andere gevallen niet.

3.3.2.7 De procedures voor omgang met datalekken

Medewerkers hebben een redelijk beeld van wanneer sprake is van een inbreuk of incident met persoonsgegevens. De 'knop' op huisnet is niet bij iedereen bekend

De medewerkers die wij hebben gesproken bleken een goed beeld te hebben van wanneer sprake was van een inbreuk of incident met persoonsgegevens. De vraag hoe daarna moest worden gehandeld en in het bijzonder de 'knop' op het huisnet waarmee datalekken gemeld kunnen worden bleek bij de meesten bekend te zijn, maar niet bij iedereen. Op zich is dat geen groot probleem omdat er meerdere andere mogelijkheden bestaan om een melding te doen, waaronder het rechtstreeks melden bij de CISO of privacy officer, die voor iedereen bekend zijn of snel te vinden.

Er blijken in de praktijk maar weinig meldingen te worden gedaan. Zie ook punt 3.4.2.8.

De processen voor het afdoen van datalekken zijn beschreven

Met de overgang van het centrale incidenten (inclusief datalekken) naar de ICT-dienstverlener 'ICT Noord- en Midden-Limburg' (ICTNML) vindt het eerste deel van het afhandelingsproces van datalekken na de melding plaats bij ICTNML, die daarvoor duidelijke procedures heeft opgesteld. In het geval van datalekken, wordt vanuit dit proces een melding gedaan aan de privacy officer van de gemeente Nederweert. Vanaf dat punt treedt de interne 'Procedure beveiligingsincidenten en datalekken gemeente Nederweert' in werking, die ook voldoende is beschreven.

Afwegingskaders voor melding aan AP en betrokkenen zijn beschreven, echter incorrect

In de 'Procedure beveiligingsincidenten en datalekken gemeente Nederweert' is een stappenplan opgenomen die de FG samen met de CISO / Privacy officer doorneemt om aan de hand van diverse criteria te bepalen of een melding aan de AP noodzakelijk is. Daarbij wordt alleen melding gedaan bij de AP indien sprake is geweest van een opzettelijke inbreuk op de beveiligingsmaatregelen. Dit zou inhouden dat geen melding aan de AP wordt gedaan indien per abuis grote hoeveelheden persoonsgegevens worden gelekt.

Ten aanzien van het melden van een datalek aan betrokkenen vermeldt de procedure vermoedelijk per abuis dat als de vraag of er ernstige gevolgen voor de privacy van de betrokkenen *negatief* wordt beantwoord een datalekmelding aan betrokkenen moet worden gedaan.

Meldingen van (mogelijke) privacyschendingen die als klacht binnenkomen worden niet doorgeleid naar de datalekprocedure

Tijdens het onderzoek is ons opgevallen dat diverse meldingen van (vermeende) privacyschendingen door middel van de klachtenprocedures aan de gemeente zijn gedaan. Deze meldingen werden volgens de klachtenprocedure afgedaan en bleken niet doorgeleid te worden naar de privacy officer of de FG. Daarmee bleven de meldingen buiten het zicht van deze functionarissen. Ofschoon de aard van de betreffende klachten hoogstwaarschijnlijk niet zouden

hebben geleid tot een datelekmelding, is door het ontbreken van een koppeling tussen de klachtenprocedure en de datalek procedure de kans aanwezig dat klachten die wel (binnen 72 uur) tot een datalekmelding zouden moeten leiden eveneens buiten het zicht van privacy officer en FG blijven.

De tijdige melding van datalekken aan AP lijkt te zijn gewaarborgd

Met uitzondering van de situatie als hierboven geschetst, lijkt de datalekprocedure zodanig te zijn georganiseerd dat wanneer nodig een tijdige melding aan de AP gewaarborgd is. Alle relevante actoren bij de gemeente zijn zich bewust van het belang en hebben bovendien een WhatsApp groep opgericht om elkaar indien nodig snel te kunnen 'alarmeren'.

Een crisiscommunicatieplan is niet beschikbaar, maar wordt ook niet nodig geacht

De gemeente Nederweert heeft geen crisiscommunicatieplan opgesteld voor het geval zich datalekken met een hoge impact voordoen. Op directieniveau wordt dit niet nodig gevonden, mede omdat op korte termijn de benodigde mensen bij elkaar kunnen komen, er bij de veiligheidsregio wel een plan ligt (maar niet volledig uitgeschreven) en de provincie Limburg hulp heeft aangeboden bij dergelijke incidenten.

Afspraken met de raad over hun betrokkenheid bij datalekken zijn niet gemaakt

Met de raad zijn geen afspraken gemaakt over of en zo ja, wanneer en hoe deze wordt geïnformeerd in het geval van datalekken. In de procedures voor het omgaan met datalekken wordt hier (dan ook) geen aandacht aan besteed.

3.3.2.8 De afhandeling van eerdere privacyschendingen/datalekken

Het beperkte aantal meldingen is naar behoren afgehandeld

Sinds de implementatie van de AVG hebben zich bij de gemeente Nederweert voor zover ons bekend slechts een beperkt aantal privacyschendingen/datalekken voorgedaan. Voor zover we hebben kunnen nagaan, zijn deze allen op juiste wijze afgehandeld.

3.3.2.9 De vereiste toestemming lijkt te worden geregistreerd

Voor veel van de persoonsgegevens die de gemeente verwerkt is geen toestemming van betrokkenen vereist omdat dit plaats vindt op grond van wettelijke bepalingen. Op basis van enkele voorbeelden in het sociale domein waar toestemming vereist is om gegevens te delen, hebben wij vernomen dat de toestemming wordt gevraagd en vastgelegd in het dossier van betrokkenen, bijvoorbeeld in de overeenkomst voor WMO. Telefonische verkregen toestemming wordt vastgelegd in het dossier, maar niet meer teruggekoppeld naar de burger.

Het is op basis van de informatie de we hebben gekregen niet mogelijk te concluderen dat de vereiste toestemming in alle gevallen gemeentebreed wordt verkregen en geregistreerd, maar we stellen vast dat het bij een van de privacy-gevoelige domeinen nadrukkelijk de aandacht heeft en er zorgvuldig mee wordt omgegaan.

3.3.2.10 Procedures voor afhandeling verzoeken rechten betrokkenen slechts beperkt aanwezig en betrokkenen niet adequaat geïnformeerd

In de privacyverklaring van de gemeente Nederweert zijn de rechten van betrokkenen opgesomd en kort beschreven. Daarbij is ook aangegeven dat om gebruik te maken van deze rechten een verzoek moet worden ingediend en dat het verzoek schriftelijk kan worden ingediend. Ook is aangegeven dat de gemeente binnen vier weken na ontvangst van het verzoek zal beoordelen of het verzoek gerechtvaardigd is en dat indien het verzoek niet wordt opgevolgd de mogelijkheid bestaat om bezwaar te maken bij de gemeente of een klacht in te dienen bij de AP.

Voor twee van de 'rechten' hebben wij een procedure gezien. Het betreft het correctierecht en het inzagerecht. Opvallend genoeg zijn ook de enige twee rechten die – als voorbeeld – in het externe privacybeleid van de gemeente staan vermeld. Voor de overige rechten (het recht op informatie, verwijderen van gegevens, beperking van de verwerking, dataportabiliteit, bezwaar en recht op een menselijke blik bij besluiten) konden ons geen procedurebeschrijvingen worden getoond.

Uit (de onderleggers bij) het jaarverslag van de FG blijkt dat betrokkenen voorafgaand aan de verwerking mogelijk niet voldoende actief, tijdig en adequaat worden geïnformeerd. Informatiefolders ontbreken, er is niet vastgesteld of uit aanvraagformulieren duidelijk wordt welke gegevens worden verwerkt noch of betrokkenen op andere wijze geïnformeerd worden.

3.3.2.11 Geautomatiseerde beslissingen vinden niet plaats

Ons is verteld dat geen geautomatiseerde beslissingen plaatsvinden bij de gemeente Nederweert. Hierdoor zijn de additionele eisen die aan dergelijke algoritmes worden gesteld op het gebied van de gegevensbescherming op dit moment niet van toepassing.

3.3.2.12 Borging gegevensbescherming in samenwerkingsverbanden

Het is voor betrokkenen onduidelijk aan welke samenwerkingsverbanden de gemeente deelneemt en hoe de afspraken daarbij zijn over het omgaan met persoonsgegevens

Gemeenten nemen vaak deel aan samenwerkingsverbanden. Daarin werken zij samen met andere (semi)overheidspartijen en/of marktpartijen, zoals de politie, andere gemeenten, het Openbaar Ministerie en uitvoeringsorganisaties, maar ook aan maatschappelijke organisaties en bijvoorbeeld zorgpartijen en woningcorporaties.

Samenwerkingsverbanden verschillen onderling sterk. Er zijn verschillen in het doel van het samenwerkingsverband, de partijen die meedoen en de taken waarvoor zij samenwerken. Deze kenmerken zijn bepalend voor de vraag of persoonsgegevens worden gedeeld en zo ja, hoe dat gebeurt en om welke gegevens het gaat.

Burgers zijn doorgaans niet goed op de hoogte van de verwerking van hun persoonsgegevens door samenwerkingsverbanden. Dit zou wel zo moeten zijn.

Volgens de autoriteit Persoonsgegevens stelt de privacywetgeving extra eisen bij complexe verwerkingen waarbij veel organisaties betrokken zijn. De gemeente moet burgers in begrijpelijke taal informeren over het samenwerkingsverband en de verwerking van hun persoonsgegevens

daarbinnen. Dit geldt nog sterker als via het samenwerkingsverband een ingrijpende beslissing over een burger wordt genomen. Bijvoorbeeld of deze burger wel of niet voor hulp of ondersteuning in aanmerking komt.

Zoals al vermeld in punt 3.3.2.1, ontbreken bij het verwerkingsregister onder meer de de namen en contactgegevens van andere organisaties met wie de gemeente gezamenlijk de doelen van en middelen voor de verwerking heeft vastgesteld (gezamenlijke verantwoordelijkheid). Ook is het voor de betrokkenen in Nederweert niet eenvoudig zich een beeld te vormen van andere samenwerkingsverbanden waar de gemeente deel van uitmaakt en die mogelijk hun persoonsgegevens verwerken. In het verwerkingsregister staan partijen met wie de gemeente samenwerkt soms direct als verwerker benoemd, maar ook vaak als 'ontvanger' van de gegevens. Doordat één partij betrokken kan zijn bij meerdere verwerkingen, is dat beeld versnipperd. Daarnaast komen diverse samenwerkingsverbanden waaraan de gemeente deelneemt in het geheel niet voor in het verwerkingsregister. Omnibuzz is een voorbeeld daarvan.

Ook is niet altijd duidelijk hoe precies de verantwoordelijkheden op het gebied van gegevensbescherming in het samenwerkingsverband zijn belegd. Een recent voorbeeld daarvan is de 'samenwerkingsverband Same Ein'. Dit is een samenwerkingsverband van tien maatschappelijke organisaties, waaronder de gemeente Nederweert, die de handen ineen hebben geslagen om hun dienstverlening nog beter af te stemmen op de vragen van inwoners uit Gemeente Nederweert. Het samenwerkingsverband heeft een eigen website waar mensen een vraag kunnen stellen of een terugbel verzoek kunnen doen. Daarbij moeten persoonsgegevens ingevuld worden. De website kent geen privacyverklaring, waardoor het onduidelijk is hoe met deze persoonsgegevens wordt omgegaan. Wat de rol van de gemeente in dit samenwerkingsverband is wordt ook niet duidelijk. Het is niet inzichtelijk hoeveel andere, wellicht vergelijkbare samenwerkingsverbanden er zijn waaraan de gemeente deelneemt.

3.4 De menselijke factor

3.4.1 Inleiding

Algemeen

De 'menselijke factor' wordt breed gezien als een van de kritische succesfactoren als het gaat om gegevensbescherming. De technische en organisatorische maatregelen die een organisatie kunnen nog zo goed zijn, als onvoldoende aandacht wordt besteed aan de mensen die met de gegevens omgaan, ligt een datalek al snel op de loer. Volgens de begroting 2024 van de gemeente Nederweert staat onder de kop 'Informatieveiligheid en Privacy' vermeld dat in 95% van de beveiligingsincidenten en datalekken de menselijke factor vaak de oorzaak is.

Diepgang en scope onderzoek naar de menselijke factor

De 'menselijke factor' is een breed begrip en niet altijd even grijpbaar begrip. Het gaat over zaken als 'de cultuur' van de organisatie en komt uiteindelijk tot uitdrukking in het gedrag van individuen en groepen in de organisatie. Het is echter lastig te meten en te sturen. Juist deze combinatie van het belang van de menselijke factor voor de gegevensbescherming en het meer diffuse karakter ervan, heeft ons ertoe gebracht aan dit onderwerp relatief veel aandacht te besteden. Daarbij hebben wij de acht cultuurdimensies uit het gedachtegoed over 'Soft Controls' van [redacted] / KPMG in het

normenkader verwerkt. Soft controls zijn alle niet-tastbare maar wel gedrag beïnvloedende factoren in organisaties die kunnen helpen bij het realiseren van doelen en het managen van risico's. Hoe prominenter deze zogenoemde soft controls in een organisatie aanwezig zijn, des te groter is de kans op gewenst gedrag en des te kleiner de kans op risico's en incidenten.

Hierna gaan wij in op onze bevindingen op het gebied van de menselijke factor.

3.4.2 Bevindingen ten aanzien van de menselijke factor

3.4.2.1 Helderheid

Het privacybeleid en het belang ervan zijn helder en duidelijk genoeg

Uit onze gesprekken met zowel MT, teamleiders en medewerkers blijkt dat het beleid op het gebied van de gegevensbescherming over het algemeen voldoende bekend is. Ook het belang van gegevensbescherming en de daarvoor geldende regels zijn bij iedereen duidelijk. De verplichte introductiebijeenkomsten voor nieuwe medewerkers waarin aandacht wordt besteed aan het onderwerp en de gesprekken met de teamleiders en onderling binnen de teams hierover dragen in belangrijke mate bij aan deze duidelijkheid.

Medewerkers lijken goed op de hoogte te zijn van hoe en waar privacy een rol speelt in hun werkprocessen. Sommige domeinspecifieke IT systemen kennen eigen verplichte e-learning modules op onder andere het gebied van privacy, waarmee de extra kennis en bewustzijn wordt gecreëerd.

Concrete voorbeelden van casussen waarbij het niet goed is gegaan, met name dichtbij binnen de eigen of andere teams binnen de gemeente, worden besproken met als doel ervan te leren.

De behoefte aan opfrissing bij personeel is meermalen benoemd

Waar nieuwe medewerkers tijdens de introductie goed worden geïnformeerd over hoe met gegevensbescherming omgegaan dient te worden, is voor het personeel dat al wat langer werkzaam is bij de gemeente niet voorzien in gestructureerde periodieke opfrissing van de kennis. Tijdens de interviews is door medewerkers meermaals de behoefte daaraan geuit. De CISO heeft aangegeven dat het inderdaad de bedoeling is dit te organiseren, maar dat heeft nog niet plaatsgevonden. In gesprekken met zowel MT-leden als de OR is de Nederweert Academy ter sprake gekomen, waarbij verschillende thema's aan bod komen, werd gesuggereerd dat gegevensbescherming daar ook onderdeel van zou kunnen uitmaken.

Gegevensbescherming wordt van hoog tot laag serieus genomen

In alle gesprekken hebben wij de indruk gekregen dat de gesprekspartners het onderwerp gegevensbescherming erg serieus nemen.

Er is een regeling gedragscode waarin ook gegevensbescherming aandacht krijgt

Hoofdstuk 12 van het Personeelshandboek van de gemeente Nederweert is de "Regeling gedragscode werknemers". In artikel 12 van die regeling ('vertrouwelijk omgaan met gevoelige informatie') worden onder andere op hoofdlijnen het zorgvuldig omgaan met persoonlijke gegevens van burgers en het respecteren van de privacy van burgers, cliënten, zakelijke relaties en collega's

benoemd als integer gedrag. Het artikel noemt ook het niet lekken van vertrouwelijke informatie, het veilig opbergen/afschermen van vertrouwelijke informatie en het afsluiten of vergrendelen van de computer bij het verlaten van de werkplek. Dit draagt op praktische wijze bij aan de helderheid van welk gedrag wordt verwacht van de medewerkers.

3.4.2.2 Voorbeeldgedrag ('tone at the top')

Het voorbeeldgedrag in de organisatie roept een wisselend beeld op

Voorbeeldgedrag door de leidinggevenden in de organisatie is van groot belang. Goed voorbeeld doet immers goed volgen. Niet alleen wat de leidinggevenden zeggen en doen is belangrijk, maar ook wat ze niet zeggen of niet doen.

In dat verband zien we dat, zoals hiervoor vermeld, de leidinggevenden allen uitdragen dat gegevensbescherming belangrijk is en er in termen van beschikbare personele capaciteit, zowel formatief als ingehuurd, ook serieus werk van maken.

Ook hebben we verschillende concrete voorbeelden gehoord van hoe leidinggevenden zelf omgaan met privacyvraagstukken binnen hun team, zoals rond ziekteverzuim van collega's. Daarmee laten ze duidelijk merken het onderwerp zelf ook met de nodige zorgvuldigheid te behandelen.

Tegelijk zijn er zaken die, zeker in samenhang, het beeld in de organisatie kunnen oproepen dat het management het onderwerp mogelijk minder belangrijk vindt. Hierbij kan gedacht worden aan:

- het gegeven dat het interne privacybeleid bijna een jaar is verlopen voordat zeer recent aan een nieuwe versie is begonnen;
- het interne privacybeleid dat vier jaar lang als concept gepubliceerd is geweest;
- onderdelen van het beleid die na vaststelling niet zijn uitgevoerd;
- het aantal DPIA's dat sterk achterblijft en er geen concreet plan is hoe dat op te lossen;
- het systeem van privacybeheerders dat al enkele jaren in de praktijk niet goed van de grond komt;
- het feit dat een speerpunt op dit vlak in de begroting is opgenomen, waarvoor geen concreet plan lijkt te zijn gemaakt waarvan geen voortgangsmeldingen worden gedaan of gevraagd;
- dat de gemeenteraad anders dan via een incidentele themaraad in 2023 niet structureel over de stand van zaken rondom de gegevensbescherming wordt geïnformeerd en bijvoorbeeld niet wordt betrokken bij de jaarrapporten van de FG;
- dat door verschillende betrokkenen wordt gesteld dat rondom gegevensbescherming een 'piepsysteem' wordt gehanteerd.

3.4.2.3 Betrokkenheid

Medewerkers worden en zijn doorgaans voldoende betrokken

Uit de gesprekken die we hebben gevoerd met leidinggevenden en medewerkers van de twee teams die het meest met (bijzondere) persoonsgegevens te maken hebben leiden we af dat de medewerkers zowel door de managers als uit zichzelf goed betrokken zijn bij de privacybescherming. Bij de

invulling van het beleid, de werkprocessen en -procedures worden de medewerkers voldoende meegenomen en denken ze nadrukkelijk mee. Hun ideeën, suggesties en opmerkingen ook op het gebied van de gegevensbescherming worden serieus genomen. Zoals eerder vermeld, worden ook casussen waar iets fout is gegaan binnen eigen of andere teams in Nederweert met elkaar gedeeld en besproken wat niet alleen leerzaam is, maar ook de betrokkenheid verder vergroot.

3.4.2.4 Uitvoerbaarheid

Soms wordt het privacybeleid als hinderlijk ervaren, maar wel als noodzakelijk en uitvoerbaar.

Tijdens meerdere gesprekken is ons verteld dat de regels omtrent de privacybescherming het werk voor de medewerkers bemoeilijkt. Daarbij komt naast de vele vereiste vastleggingen en verantwoording ook het gevoel naar voren dat de regels het moeilijk maken de cliënten goed te helpen. Desondanks geeft iedereen met wie wij hebben gesproken ook aan te begrijpen dat de regels er niet voor niets zijn, deze te onderschrijven en ze ook uit te kunnen voeren.

Werkdruk en druk vanuit college worden gezien als risico voor fouten

Ofschoon in het algemeen de regels omtrent gegevensbescherming zoals hiervoor gesteld uitvoerbaar worden geacht, wordt in enkele gevallen wel een zodanige werkdruk en druk vanuit het college ervaren dat een verhoogde risico op fouten – ook op het gebied van privacybescherming – wordt gezien.

Kantoortuin concept met flexplekken biedt voordelen, maar ook risico's

Uit de interviews hebben wij begrepen dat medewerkers van het sociale domein in een kantoortuin omgeving werken, met flexplekken die ook beschikbaar zijn voor medewerkers en ingehuurde krachten van andere teams. Wij realiseren ons dat dit een efficiënte manier is om de kostbare werkplekken optimaal te benutten. Tegelijkertijd brengt dit concept ook een verhoogd risico op privacyschendingen met zich mee, ook al tracht het team zoveel mogelijk gevoelige gesprekken in afgesloten (vergader) ruimtes te voeren.

3.4.2.5 Bespreekbaarheid

Voldoende randvoorwaarden om gegevensbescherming bespreekbaar te maken zijn aanwezig

Voor zover wij kunnen nagaan, zijn voldoende randvoorwaarden aanwezig om het onderwerp gegevensbescherming bespreekbaar te maken en te houden. Medewerkers zijn in grote lijnen op de hoogte van wat een datalek is en weten hoe ze die moeten melden of kunnen daar zeer eenvoudig achter komen. Ook hebben wij gemerkt dat er een vrij open, professionele opstelling is bij de teams waarmee we hebben gesproken die bijdraagt aan de bespreekbaarheid. Vragen, dilemma's en mogelijke 'grijze gebieden' worden onderling en in teamverband besproken, soms met ondersteuning van de privacy officer. Bevindingen bij audits, zoals op SUWINet worden teruggekoppeld aan betrokkenen. Incidenten bij andere gemeenten en instellingen die het nieuws halen, worden niet structureel besproken.

Voor het geval toch twijfels zouden bestaan over de mogelijkheid om veilig misstanden, waaronder ook schendingen van de privacyregels, te kunnen melden, heeft de gemeente Nederweert bovendien in hoofdstuk 13 van het Personeelshandboek een klokkenluidersregeling opgenomen ('Regeling melden vermoeden misstand en inbreuk op Unierecht'). Punt van aandacht hierbij is dat deze regeling geen grote bekendheid lijkt te genieten binnen de gemeente.

3.4.2.6 Aanspreekbaarheid

Medewerkers en managers lijken aanspreekbaar op hun gedrag. Er wordt voldoende ruimte ervaren om kritiek te uiten

Op basis van de in de gesprekken ervaren open en professionele opstelling is ons beeld dat medewerkers en managers voldoende ruimte ervaren om kritiek te uiten en aanspreekbaar zijn op hun gedrag. Tijdens de interviews werd geschetst hoe binnen teams ongewenst gedrag informeel onder elkaar wordt besproken, maar ook dat het een onderwerp kan zijn in functioneringsgesprekken.

3.4.2.7 Handhaving

Over handhaving bij overtreding van privacyregels bestaat een divers beeld

De privacy officer en diverse leidinggevenden benadrukken dat positief wordt omgegaan met medewerkers die een datalek melden, ook als zij de veroorzaker zijn. Tijdens de introductiebijeenkomsten voor nieuwe medewerkers wordt het belang van het melden benadrukt en wordt hen verteld dat het melden van een datalek geen repercussies heeft voor de melder. Melders worden gecomplimenteerd als ze een datalek melden. Bij incidenten (al dan niet als datalek gemeld) worden met de betrokkenen hierover wel gesproken.

Het contract van een ingehuurde medewerker ná een beveiligingsincident is niet verlengd, is ons tijdens een interview, na achteraf bleek onterecht, verteld. We kunnen niet inschatten in hoeverre het bij ons onterecht geschetste beeld breder in de organisatie leeft en daarmee de uitgezette lijn (leren en meldingen stimuleren) verstoort.

3.4.2.8 Transparantie

Het aantal meldingen van incidenten is onrealistisch laag. Het zicht op incidenten is hierdoor in de hele organisatie beperkt

Veel van de hiervoor in deze paragraaf behandelde onderwerpen schetsen een vrij positief beeld van de cultuur in de organisatie als het gaat om gegevensbescherming. Desondanks bestaat bij alle direct betrokkenen het beeld dat in 2024 het aantal meldingen van incidenten onrealistisch laag is gelet op de omvang en aard van de organisatie en het aantal meldingen in de jaren ervoor.

Wij hebben geen verdergaand onderzoek kunnen doen naar de oorzaken van deze vermoedelijke terugloop in meldingsbereidheid. In theorie kan dit komen doordat het aantal incidenten echt sterk is afgenomen, maar algemeen wordt aangenomen dat het aantal meldingen achterblijft. Dat zou betekenen dat in de organisatie maar beperkt zicht is op incidenten.

3.5 De organisatorische en technische maatregelen

3.5.1 Inleiding

Algemeen

Voor het beveiligen van de aan de gemeente toevertrouwde persoonsgegevens, vereist de AVG dat aantoonbaar 'passende' technische en organisatorische maatregelen worden genomen. Op dit vlak bestaat een onlosmakelijk verband tussen het beschermen van de persoonsgegevens en de algemene informatiebeveiliging van de gemeente. De bescherming van de persoonsgegevens steunt daarbij in hoge mate op de technische en organisatorische maatregelen die zijn getroffen in het kader van de informatiebeveiliging in algemene zin. Op onderdelen zullen daarnaast enkele specifiek op de bescherming van de persoonsgegevens toegespitste maatregelen noodzakelijk zijn.

Diepgang en scope onderzoek naar de organisatorische en technische maatregelen

Tijdens de oriënterende fase van het onderzoek, hebben wij ons een eerste beeld gevormd van de manier waarop bij de gemeente Nederweert de informatiebeveiliging in het algemeen is georganiseerd. Dat beeld was voor ons positief genoeg om ons te doen besluiten dit onderdeel in de uitvoeringsfase minder diepgaand te onderzoeken.

Op basis daarvan hebben wij ons qua technische maatregelen beperkt om een beeld op hoofdlijnen te krijgen van de stand van informatiebeveiliging.

Daarnaast hebben we bij de teams die het meest met (bijzondere) persoonsgegevens omgaan, op een aantal essentiële deelgebieden extra onderzoek gedaan, zowel op technisch als op organisatorisch gebied.

Onze bevindingen treft u in de paragraaf hierna aan.

3.5.2 Bevindingen ten aanzien van de organisatorische en technische maatregelen

Er is informatiebeveiligingsbeleid. Deze is versnipperd.

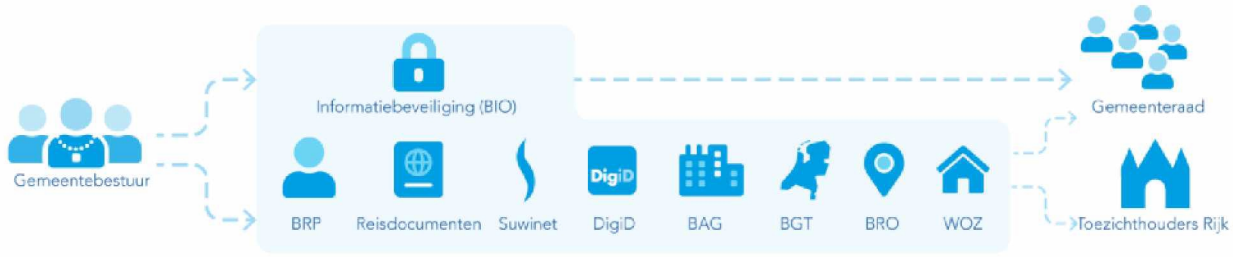
De gemeente Nederweert heeft informatiebeveiligingsbeleid. Het beleid is echter versnipperd over een aantal documenten. Het 'Strategisch Gemeentelijk Informatiebeveiligingsbeleid Nederweert 2023 tot 2024' vormt de kern. Daarin is echter aangegeven dat naast dit beleidsstuk het informatiebeveiligingsbeleid 2018 – 2020 voorlopig actief blijft wat betreft de tactische onderdelen tot die individueel zijn uitgewerkt in aparte (tactische) beleidsnota's. Daarnaast is een document 'Informatiebeveiliging Governance' vastgesteld dat een verdere uitwerking is van het strategisch informatiebeveiligingsbeleid. Het omvat afspraken, richtlijnen, procedures en verantwoordelijkheden die nodig zijn om de vertrouwelijkheid, integriteit en beschikbaarheid van (gevoelige) informatie te waarborgen.

Een overkoepelend beeld van de situatie van de informatiebeveiliging ontbreekt. De verantwoording aan de raad over de informatiebeveiliging is incompleet.

Wij hebben getracht een beeld op hoofdlijnen te vormen van de situatie van de informatiebeveiliging bij de gemeente Nederweert. Volgens het het governance beleid rondom informatiebeveiliging wordt elk jaar de raad op de hoogte gebracht over de stand van zaken rondom de informatiebeveiliging binnen gemeente Nederweert en rapporteert de gemeente over de informatieveiligheid van de gemeente in de jaarrekening.

Zowel de structurele informatieverstrekking aan de raad over de stand van de informatiebeveiliging, als de informatie die in de jaarrekening is opgenomen is gebaseerd op de (verplichte) systematiek van de Eenduidige Normatiek Single Information Audit (ENSIA).

De figuur hierna maakt duidelijk dat met behulp van deze methodiek over twee aspecten van de informatiebeveiliging verantwoording wordt afgelegd aan de gemeenteraad. Enerzijds betreft het de algemene toestand van de informatiebeveiliging bij de gemeente op basis van de Baseline Informatiebeveiliging Overheid (BIO), zoals weergegeven in de bovenste helft van de figuur. Anderzijds betreft het informatie over een aantal landelijke voorzieningen waarover de gemeente verantwoording af moet leggen, zoals weergegeven in de onderste helft van de figuur.



Op basis van de ENSIA methodiek zou dus een goed en vrij integraal beeld moeten ontstaan bij de gemeenteraad over de mate waarin over de wijze waarop de gemeente in control is op het thema ‘informatieveiligheid’.

Wij constateren dat in de Raadsinformatiebrief over ENSIA 2023 (nr. RIV-24-00842 d.d. 10-4-2024) uitsluitend betrekking heeft op het onderste deel van de figuur hierboven. Uit deze toets volgen geen bevindingen. De uitkomsten van de toets van alle andere facetten van de gemeentelijke informatiebeveiliging (het bovenste deel van de figuur) ontbreken geheel.

De ENSIA biedt gemeentes ruimte om, op basis van eigen (risico-)afwegingen de reikwijdte van de jaarlijkse verantwoording te bepalen. In de interviews die we hebben gehouden is ons verteld dat de gemeente twaalf bedrijfskritieke applicaties heeft geïdentificeerd die worden meegenomen in de ENSIA, evenals alle applicaties die met Digid en Suwinet werken. Waarom dit niet tot uitdrukking komt in de (ENSIA)verantwoording naar de raad is ons niet duidelijk.

In de jaarrekening 2023 nemen wij hetzelfde beeld waar. In het onderdeel ‘Privacy en Informatiebeveiliging’ van de paragraaf ‘Informatisering en automatisering’ staat dat het bestuur jaarlijks verantwoording aflegt over informatieveiligheid aan zowel de (gemeente)raad als nationale toezichthouders en dat die verantwoording wordt gedaan binnen het ENSIA-verantwoordingsproces. Daarna vermeldt het betreffende onderdeel van de jaarrekening echter enkel dat op basis van de ENSIA-verantwoording van 2023 het college van burgemeester en wethouders heeft bevestigd dat de gemeente Nederweert op 31 december 2023 voldoet aan de vastgestelde normen en eisen van DigiD en Suwinet en dat de resultaten van de externe IT-audit

voor DigiD en Suwinet deze conclusie bekrachtigen. Over de generieke informatiebeveiliging bij de gemeente wordt ook hier met geen woord gerept. Wij hebben geen andere documenten gevonden waarin daarover verantwoording wordt afgelegd. Het is naar ons oordeel voor de raad niet mogelijk om zich een goed beeld te vormen van de stand van zaken op basis van deze onvolledige informatie.

Op DigiD en Suwinet na, vindt de gehele ENSIA plaats op basis van zelfevaluatie

Ten aanzien van de domeinen DigiD en Suwinet dient het college een verklaring op te stellen, waarin zij verklaart in welke mate de gemeente voldoet aan de informatiebeveiligingsnormen. Het is daarna verplicht om een bij de NOREA geregistreerde IT-auditor de Collegeverklaring te laten controleren. De IT-auditor verklaart in het Assurancerapport dat de Collegeverklaring een getrouw beeld geeft. Getrouw betekent dat de Collegeverklaring met een redelijke mate van zekerheid juist en volledig is. Deze verklaring van getrouwheid geeft aanvullende zekerheid over de juistheid en volledigheid van de Collegeverklaring.

Het staat gemeenten volgens het ENSIA verantwoordingsstelsel vrij om ook andere onderdelen van ENSIA verantwoording te laten onderzoeken door een IT-auditor; hiertoe is geen verplichting. De gemeente Nederweert maakt noch structureel, noch incidenteel gebruik van deze mogelijkheid, waardoor alle onderdelen van de ENSIA verantwoording met uitzondering van DigiD en Suwinet al jarenlang enkel tot stand komen op basis van zelfevaluatie.

Zicht op informatiebeveiliging bij verwerkers en samenwerkingsverbanden wisselt

Als het gaat om het in beeld krijgen en houden van de kwaliteit van de informatiebeveiliging bij derden aan wie de gemeente persoonsgegevens toevertrouwt, zien we een wisselend beeld. Van sommige partijen, zoals ICT NML wordt een zogenaamde Third Party Mededeling gevraagd, waarin een onafhankelijk audit partij een verklaring afgeeft over de kwaliteit van een ICT-dienstverlening en – beheersing van een organisatie. Hiermee wordt een redelijke mate van zekerheid verkregen in hoeverre aan de norm wordt voldaan (in het geval van ICT NML is de norm de Baseline Informatiebeveiliging Overheid). De [redacted] komt tot een aantal bevindingen voor zowel de ICT-organisatie als de gemeenten. De bevindingen betreffen niet alleen privacy-aspecten. Bevindingen met betrekking tot autorisaties en bewaartermijnen sluiten aan bij de bevindingen van de Rekenkamer. Van een aantal bevindingen uit de TPM is op basis van het bestudeerde rapport niet helder of deze al dan niet betrekking hebben op privacy-aspecten.

In andere gevallen wordt, zoals reeds in punt 3.3.2.5 is vermeld weinig tot niets gedaan om de kwaliteit van de informatiebeveiliging te toetsen en wordt meer op vertrouwen gevaren. Wij zijn geen risico-afweging tegengekomen op basis waarvan is besloten wanneer wel en wanneer geen nader onderzoek nodig is.

Vertrouwelijke stukken over informatiebeveiliging waren openbaar

Tijdens ons onderzoek hebben wij op het publieksdeel van iBabs diverse vertrouwelijke bijlagen aangetroffen die horen bij de Raadsinformatiebrieven over ENSIA uit 2021 en 2022, terwijl in de Raadsinformatiebrieven zelf nadrukkelijk is vermeld dat het in het kader van informatiebeveiliging niet wenselijk is dat de details van de ENSIA audit openbaar zijn en daarom de bijlagen bij de raadsinformatiebrief vertrouwelijk voor de raad ter inzage worden gelegd.

Direct na ontdekking hiervan hebben wij dit gemeld bij de raadsgriffier, die binnen de gemeente ervoor heeft laten zorgen dat de betreffende documenten alsnog zijn verwijderd.

Autorisatiebeheer is geregeld, maar kan op onderdelen beter

Toegangsrechten voor medewerkers worden toegekend aan de hand van het functieprofiel. Eventuele noodzakelijke aanpassingen vinden plaats met behulp van een autorisatieformulier.

De gemeente gebruikt een zaak-systeem, JOIN, waarin alle dossiers worden opgeslagen. Toegang tot de dossiers wordt verleend op basis van autorisatietabellen in JOIN. De autorisatietabellen worden beheerd door de beheerder van JOIN.

Toegang aan gebruikers wordt verleend aan de hand van eerder aan andere gebruikers met vergelijkbare functies toegekende autorisaties of gebaseerd op beschrijvingen van de werkprocessen in het door de VNG opstelde document I-Navigator. De beheerder van JOIN hanteert geen formeel vastgesteld document over toe te kennen rechten. De toekenning van rechten in JOIN zoals dat nu gebeurt kan strikter.

Logging vindt plaats bij de teams met de meeste (bijzondere) persoonsgegevens

Zowel in het sociale domein als bij publiekszaken is ons verteld dat gebruik wordt gemaakt van logging. Daarmee worden in computersystemen gebeurtenissen die belangrijk zijn voor de beveiliging of voor de analyse van verstoringen in een logbestand vastgelegd.

De logging wordt achteraf bekeken en opvallende zaken worden aan de teamleider gemeld. Na verdere analyse wordt indien nodig de desbetreffende medewerker om uitleg gevraagd.

De teamleden uit de betreffende teams lijken goed op de hoogte van deze werkwijze, waardoor er ook een preventieve werking vanuit gaat. Het ingeziene rapport over onderzoek naar (de gelogde) toegang van persoonsgegevens in Suwinet is helder en vertrouwenwekkend.

Sterke wachtwoorden en frequente vernieuwing worden veelal afgedwongen

De gemeente maakt voor het inloggen gebruik van Azure. Daarmee wordt het instellen van sterke wachtwoorden en regelmatige vernieuwing dan het wachtwoord afgedwongen. Niet alle applicaties maken gebruik hiervan. Sommige applicaties kennen een eigen password policy. In het financiële systeem leidde dit tot bemerkingen van de accountant.

Van medewerkers uit het sociale domein vernamen we dat passwords in hun beleving vaak gewijzigd moeten worden.

Er is een Controller Informatiebeveiliging. Deze is recent aangesteld.

De gemeente heeft recent een controller informatiebeveiliging aangesteld. Deze functionaris is echter pas recent begonnen in deze functie en is zich nog aan het oriënteren.

Op individueel niveau worden VOG, geheimhoudingverklaring en eed vereist

Zonder geldige VOG en geheimhoudingsverklaring kunnen mensen niet zelfstandig in backoffice van het gebouw en in de systemen van de gemeente. Daarnaast wordt ten overstaande van het volledige college de eed afgelegd. Hiermee wordt zoveel als mogelijk en toegestaan op voorhand geborgd dat op integere wijze met gegevens wordt omgegaan.

Het stelsel van privacy-ambassadeurs functioneert niet optimaal

De gemeente heeft een aantal jaren geleden de rol van privacy-ambassadeurs geïntroduceerd bij diverse teams. Ofschoon deze functionarissen veelal op individuele basis in positieve zin bijdragen

aan de gegevensbescherming, ontbreekt een gestructureerde aanpak, met aansturing, begeleiding en coördinatie van de activiteiten.

3.6 Het toezicht

3.6.1 Inleiding

Algemeen

De kerntaak van de FG is het houden van toezicht op de toepassing en naleving van de privacywetgeving. De naleving van de privacywetgeving is echter de verantwoordelijkheid van de gemeente zelf. Dat houdt in dat de gemeente zelf verantwoordelijk is voor het inrichten, uitvoeren, borgen en monitoren van alle onderdelen ervan, inclusief het toezicht daarop en de verantwoording daarover.

Diepgang en scope onderzoek naar het toezicht

Tijdens de oriënterende fase hebben wij kennis genomen van de wijze waarop de FG zijn toezicht op de naleving van de AVG bij de gemeente Nederweert uitvoert. Op basis daarvan hebben wij ervoor gekozen om ons tijdens de uitvoering van het onderzoek voor wat betreft toezicht voornamelijk te richten op enerzijds hoe de gemeente omgaat met de bevindingen van de FG en anderzijds hoe in de bredere planning en controlcyclus, van begroting tot en met jaarverslag het onderwerp gegevensbescherming wordt gestuurd en beheerst.

Waar wij tijdens het onderzoek nog stuitten op verbetermogelijkheden ten aanzien van het toezicht door de FG hebben we die uiteraard meegenomen in onze bevindingen.

3.6.2 Bevindingen ten aanzien van het toezicht

De FG houdt gedurende het jaar zoals vereist toezicht, met enkele uitzonderingen

Op basis van onze gesprekken met de FG van de gemeente Nederweert en op basis van de door hem uitgebrachte rapporten en adviezen, concluderen wij dat het toezicht van de FG wordt ingevuld zoals vereist. De FG brengt daarbij minimaal eens per jaar verslag uit van zijn bevindingen aan de gemeente.

Ten aanzien van het onderwerp “Triagemodel voor gegevensdeling bij meervoudig complexe casuïstiek, waarin de wet niet voorziet (sociaal domein)”, zie ook punt 3.2.2, stellen wij vast dat, ondanks de gevoeligheid van dit onderwerp de FG geen toezicht houdt op de wijze waarop hieraan in de praktijk invulling wordt gegeven.

Ook hebben wij geen toezicht gezien vanuit de FG op de naleving van elementen uit het verwerkingsregister, waaronder de bewaartermijnen of op de procedures die daarvoor eventueel worden gehanteerd.

De bevindingen van de FG worden niet met de raad gedeeld of (op een andere manier) openbaar gemaakt

De bescherming van de persoonsgegevens is een grondrecht. Desondanks stellen wij vast dat de jaarrapporten van de FG, waarin wordt beschreven in hoeverre de gemeente aan de daaraan gestelde

eisen voldoet, na behandeling in het college niet aan de gemeenteraad worden aangeboden. Ook worden deze rapporten niet openbaar gemaakt.

Planning, control en verantwoording rondom bescherming persoonsgegevens is mager

De verantwoording van het college en de burgemeester aan de gemeenteraad over de uitvoering van het privacybeleid is volgens het 'interne' privacybeleid geborgd in de P&C-cyclus en verloopt via de begroting en jaarrekening.

Voor het jaar 2024 staat in de begroting (blz. 99) het toenemen van het bewustzijn in de organisatie op het gebied van informatiebeveiliging en privacy als speerpunt benoemd. Navraag heeft geleerd dat sindsdien dit speerpunt sindsdien niet is omgezet in een concreet plan en ook niet tot uitvoering is gekomen. Over het gebrek aan voortgang ten aanzien van het speerpunt uit de begroting heeft gedurende het jaar geen formele rapportage plaatsgevonden aan het college, noch aan de raad.

Het is aan de controller om te (laten) beoordelen of de gemeente in control is en dat geldt volgens het interne privacybeleid ook voor privacy. We hebben echter geen stukken of oordelen gezien van de controller daarover. De enige plek waar in het interne controleplan 2024 van de gemeente over privacy wordt gerept is op blz. 10 onder de kop '1e lijnscontrole'. Daar wordt gesteld: "*Elk proceseigenaar heeft inzicht nodig in wat er kan fout gaan in zijn/haar processen welke maatregelen hij/zij moet treffen om te voorkomen dat deze fout wordt gemaakt. Deze interne controle in de 1e lijn moet zichtbaar geborgd zijn in het werkproces. Dit inzicht is ook belangrijk om een goede beheersing te krijgen over de beveiligings- en privacy risico's om zo datalekken te voorkomen. Het is de verantwoordelijkheid van de proceseigenaar om dit goed te organiseren en in te richten.*" Enerzijds is dan niet vreemd omdat het interne controleplan (IC-plan) volgend de inleiding grotendeels de basis is voor de toets op rechtmatigheid in de financiële administratie. Het plan heeft daardoor een sterk financiële focus.

De controller informatiebeveiliging is, zoals eerder gemeld, relatief nieuw op die positie en nog zoekende naar hoe hij zijn rol precies uit zal gaan voeren.

4 Conclusies en aanbevelingen

4.1 Conclusies

De gemeente Nederweert heeft de afgelopen jaren veel tijd, geld en energie gestoken in het op goede wijze implementeren en uitvoeren van de AVG. Dat heeft geleid tot een situatie waarin sprake is van een positief beeld ten aanzien van veel onderdelen van de AVG. Het risico op inbreuken op de privacy vanuit de gemeentelijke organisatie lijkt hierdoor op het eerste gezicht relatief gering. Desondanks kent de gemeente Nederweert nog een aantal significante kwetsbaarheden.

In de eerste plaats betreft het de kwaliteit en kwantiteit van een aantal formele maatregelen en documenten, zoals het beleid, het verwerkingsregister en de Data Protection Impact Assessments (DPIA's). Deze dienen bij te dragen aan de richting, sturing en beheersing van de gegevensbescherming en moeten, in het kader van de verantwoordingsplicht, aan de Autoriteit Persoonsgegevens (AP) kunnen aantonen dat aan de privacyregels wordt voldaan. Op dit moment schort hieraan nog het nodige.

Aanvullend biedt ook de governance rondom de gegevensbescherming ruimte voor verbetering, waaronder een grotere betrokkenheid van de gemeenteraad bij dit grondrecht van onze burgers.

Het tweede vlak waar wij kwetsbaarheden zien is de rechtmatigheid van een aantal onderdelen van het beleid. Daarbij leidt een streven naar een effectieve en efficiënte taakuitvoering ertoe dat op sommige thema's de grenzen van de AVG zijn opgezocht en naar ons oordeel zelfs (dreigen te worden) overschreden. Dat is het geval in het huidige "Privacyprotocol Ondermijning"[3] en het zogenaamde "Triagemodel voor gegevensdeling bij meervoudig complexe casuïstiek, waarin de wet niet voorziet (sociaal domein)" [4].

De gemeente Nederweert loopt hiermee risico's op hoge boetes van de AP en forse imagoschade. Dat dit risico niet mag worden onderschat, blijkt uit het recent door de AP uitgebrachte 'Sectorbeeld Overheid' waarin hij zegt hard in te zullen grijpen bij gemeenten die bij de bestrijding van criminaliteit in het fysieke domein de privacybelangen van burgers in het digitale domein onrechtmatig schenden.

Tenslotte hebben wij naast de vele positieve zaken op het gebied van de AVG bij de gemeente Nederweert bij elk van de onderzochte deelgebieden ook diverse mogelijkheden tot verbetering geïdentificeerd. Het gestructureerd aanpakken daarvan zal leiden tot verdere versterking en borging van de kwaliteit van de gegevensbescherming bij de gemeente Nederweert.

[3]Formeel bekend als 'Besluit van het college van burgemeester en wethouders van de gemeente Nederweert houdende regels omtrent privacy (Privacyprotocol Ondermijning Nederweert 2020)'.
[4]Opgenomen als bijlage 3 bij het (interne) Privacybeleid Gemeente Nederweert 2020 - 2023

4.2 Aanbevelingen

De bevindingen die we tijdens het onderzoek hebben gedaan brengen ons tot de hiernavolgende aanbevelingen.

De **aanbevelingen aan de gemeenteraad** zijn:

- Vraag het college van burgemeester en wethouders de aan hen gerichte aanbevelingen over te nemen.
- Ga na hoe u uw betrokkenheid bij dit voor de inwoners van de gemeente belangrijke grondrecht kunt versterken. Hierbij adviseren wij tenminste te : overwegen of en hoe u zich wil laten informeren over:
  - het jaarlijkse verslag van de functionaris gegevensbescherming;
  - de daaruit en uit dit rapport voortvloeiende verbeterplannen van het college en de opvolging daarvan;
  - een (beter) integraal beeld van de stand van zaken rondom de informatiebeveiliging in het kader van de ENSIA verantwoording, alsmede de daaruit voortvloeiende verbeterplannen;
  - (ernstige) datalekken .

De **aanbevelingen aan het college van burgemeester en wethouders** zijn:

- Geef het thema gegevensbescherming een nieuwe impuls, ten minste gericht op de kwaliteit en kwantiteit van de voor de verantwoordingsplicht vereiste maatregelen en documenten alsmede op het verbeteren van de governance rondom dit thema.
- Trek het huidige “Privacyprotocol Ondermijning”[5] formeel in en vervang het, indien nodig, door een versie die voldoet aan de eisen uit de AVG.
- Pas het “Triagemodel voor gegevensdeling bij meervoudig complexe casuïstiek, waarin de wet niet voorziet (sociaal domein)” aan zodat duidelijk is dat binnen de grenzen van de AVG wordt gebleven en geeft de privacy officer een adviserende rol bij de uitvoering.
- Analyseer de overige bevindingen in dit rapport zoals opgenomen in hoofdstuk 3 en bijlage 4, stel onderbouwd vast of en zo ja welke verbetermaatregelen noodzakelijk of wenselijk zijn en met welke prioriteit. Wijs deze toe aan verantwoordelijken en monitor de voortgang. Informeer in lijn met de eerste aanbeveling de gemeenteraad over de gemaakte keuzes, het verbeterplan en de voortgang daarvan.

[5]Formeel bekend als ‘Besluit van het college van burgemeester en wethouders van de gemeente Nederweert houdende regels omtrent privacy (Privacyprotocol Ondermijning Nederweert 2020)’.

5 Bestuurlijke reactie

Nederweert
samen groots, samen doen!

Gemeentehuis
Raadhuisplein 1, Nederweert

Postbus 2728
6030 AA Nederweert
T 14 0495 of (0495) 677 111
F (0495) 633 245
E info@nederweert.nl
www.nederweert.nl
NL08 BNGH 028.50.05.804

Rekenkamer
Postbus 2728
6030 AA NEDERWEERT

kenmerk : UIT-25-39638
beh. door : J.C.T. Bakens
bijlage(n) :

uw bericht :
datum : 12 februari 2025
verzonden : 12 februari 2025

onderwerp : Onderzoek rekenkamer AVG

Geachte leden van de rekenkamer,

Op de eerste plaats willen we onze erkentelijkheid uitspreken over het aangeboden conceptrapport over de naleving van de Algemene Verordening Gegevensbescherming (AVG) door de gemeente Nederweert.

Het naleven van de AVG achten wij van groot belang. Als medeoverheid behoren we wetgeving uit te voeren en na te leven. We hebben daarbij een voorbeeldfunctie die niet mag worden onderschat. Het hoofddoel van de AVG was en is immers bescherming van ieders privacy.

De toepassing van de AVG is soms lastig. Je wilt als overheid immers waar mogelijk zorgen voor een goede dienstverlening en ondersteuning aan je inwoners. Maar soms lijkt dit vanwege de stringente regels die de AVG oplegt niet mogelijk.

Uw rapport is helder opgebouwd en de gevoerde gesprekken met medewerkers en verantwoordelijk portefeuillehouder zijn vanuit een positief kritische manier gevoerd.

De AVG heeft binnen onze ambtelijke organisatie sinds de invoering van de AVG meer en meer aandacht gekregen. Daarbij stellen we hoge eisen aan de kwaliteit bij de uitvoering van werkzaamheden. Dit heeft er bijvoorbeeld toe geleid dat we de functie van privacy officer afgelopen jaar opnieuw hebben moeten openstellen. We zijn blij dat zeer recent een nieuwe medewerker is geworven op deze functie.

De aanbevelingen die u geeft aan het college van B&W zijn allen valide en nemen we graag over. Binnen het team informatievoorziening wordt gewerkt aan een plan van aanpak. We verwachten dit plan net voor de zomer aan te kunnen bieden aan de gemeenteraad. In het plan worden de diverse verbetervoorstellen geprioriteerd en van een planning voorzien.

Uw aanbevelingen aan de gemeenteraad achten wij ook relevant. Hierop zal uiteraard de gemeenteraad haar reactie geven. Wel geven wij bij deze al aan, dat wij ook deze adviezen graag een plek willen geven in het al genoemde plan van aanpak.

Ook geven wij de gemeenteraad in overweging om één keer per jaar een informatiebijeenkomst te beleggen, waarbij zaken zoals klachten, bezwaren en privacy aan de orde komen.

Dit geeft de raad ook de mogelijkheid om gerichte vragen aan het college te stellen naar aanleiding van het jaarverslag van de functionaris gegevensbescherming of informatie over mogelijke datalekken.

Mocht u naar aanleiding van onze bestuurlijke reactie vragen of opmerkingen hebben, horen we dit graag.

Met vriendelijke groet,

Burgemeester en wethouders van Nederwee

De burg

B.M.T.

6 Nawoord rekenkamer

In ons rapport stellen we vast dat de gemeente Nederweert het relatief goed doet op het gebied van de gegevensbescherming, maar dat dit niet wegneemt dat het in een aantal gevallen beter kan. De rekenkamer heeft een aantal aanbevelingen gedaan voor de raad en voor het college om invulling te geven aan die verdere verbetering.

Wij zijn blij met de bestuurlijke reactie vanuit het college van burgemeester & wethouders waarin wordt aangegeven onze aanbevelingen aan het college over te nemen. Deze positieve reactie van het college bevestigt dat het de bescherming van de aan de gemeente toevertrouwde persoonsgegevens serieus neemt. De suggestie van het college om aan de raad in overweging te geven één keer per jaar een informatiebijeenkomst te beleggen over o.a. privacy nemen we graag over.

De reactie van het college benoemt helder de spanning die het ervaart in de toepassing van de AVG en daarmee ook één van de kwetsbaarheden die de rekenkamer ziet op een aantal onderdelen van het beleid. De positieve reactie wekt sterk de verwachting dat bij toekomstige afwegingen als die spanning zich voordoet, het wettelijke privacybelang boven efficiency en effectiviteit gesteld wordt en onrechtmatigheden worden voorkomen. Expliciet wordt dit echter in de reactie niet gemaakt.

We danken de burgemeester in de rol van portefeuillehouder, de gemeentesecretaris, de geïnterviewde ambtenaren alsmede de externe adviseurs voor hun constructieve en positieve bijdrage aan het onderzoek en de heldere ambtelijke en bestuurlijke reacties op het rekenkamerrapport.

Bijlage 1 - Normenkader

1			De gemeente Nederweert beschikt over toereikend beleid ten aanzien van de AVG
	1.1		De gemeente Nederweert beschikt over beleidsdocumenten op het gebied van privacybescherming en deze zijn 'AVG-proof'.
	1.2		De gemeenteraad is voldoende betrokken (geweest) bij het formuleren en vaststellen van het beleid.

2			De gemeente Nederweert geeft voldoende invulling aan de verplichte onderdelen van de AVG
	2.1		Er is een verwerkingsregister dat voldoet aan de eisen van de AVG.
	2.2		Er is een Functionaris Gegevensbescherming en de juiste randvoorwaarden zijn aanwezig om deze voldoende te laten functioneren.
	2.3		Er is een privacyverklaring dat aan de eisen van de AVG voldoet.
	2.4		Vereiste DPIA's zijn uitgevoerd en de juistheid, volledigheid en actualiteit daarvan is geborgd.
	2.5		Waar de gemeente gebruik maakt van de diensten van verwerkers zijn daarmee verwerkersovereenkomsten getekend die voldoen aan de eisen van de AVG.
	2.6		Er is een datalekregister dat aan de eisen van de AVG voldoet.
	2.7		Er een toereikende procedure opgesteld, beschikbaar en bekend voor het conform AVG omgaan met datalekken.
	2.8		De gemeente is adequaat omgegaan met privacyschendingen/datalekken bij zichzelf en bij partners met wie op dit terrein wordt samengewerkt.
	2.9		Voor gegevens waarvoor toestemming van belanghebbende vereist is, kan deze toestemming worden aangetoond?
	2.10		Er is een procedure voor de afhandeling van verzoeken van rechten van betrokkenen (recht op informatie, inzage, rectificatie, verwijderen, beperken van de verwerking, dataportabiliteit, bezwaar en op een menselijke blik bij besluiten) en deze voldoen aan de eisen.
	2.11		Indien van toepassing: worden bij de gemeente Nederweert geautomatiseerde beslissingen genomen die voldoen aan de daarvoor geldende eisen (o.a. aandacht in DPIA voor technische aspecten, zoals algoritmekeuze, bias en NFL, transparantie en uitlegbaarheid van het algoritme en de inzet daarvan en rechten van betrokkenen, zoals het recht op verwijdering en het recht op rectificatie).
	2.12		Van persoonsgegevens die door de gemeente worden gedeeld met andere organisaties, waaronder samenwerkingsverbanden, is geborgd dat dit plaatsvindt conform de AVG.
3			Er wordt voldoende aandacht besteed aan de menselijke factor bij het beschermen van persoonsgegevens.
	3.1		**Inzicht**. Er wordt periodiek een analyse gemaakt van de grootste kwetsbaarheden (functies, processen, situaties, cultuur) op het gebied van privacybescherming en daarbij wordt voldoende aandacht besteed aan de menselijke factor.

	3.2		**Helderheid**. Medewerkers en andere personen die bij de gemeente omgaan met persoonsgegevens worden duidelijk geïnformeerd over wat van hen wordt verwacht op dat gebied. (bijv. tijdens introductieprogramma, bij betrekken andere positie, periodieke refreshers).
	3.3		**Voorbeeldgedrag**. Gedrag van het management versterkt de boodschap (of kan de boodschap ondergraven bij tegengesteld gedrag)Leidinggevenden geven in woord en daad het goede voorbeeld op het gebied van gegevensbescherming.
	3.4		**Betrokkenheid Creëren van draagvlak.** Enthousiasmeert de organisatiemanagers en -medewerkers voor de gewenste ethiek en integriteit? Of zien ze dit als een bedreiging of inperking van hun professionaliteit?
	3.5		**Uitvoerbaarheid**. Het privacybeleid en de daaraan gerelateerde processen worden als realistisch en uitvoerbaar beschouwd door de medewerkers van de gemeente
	3.6		**Transparantie** van gedrag. In hoeverre is er zicht op niet-integer gedrag? Zien managers en medewerkers de effecten van hun gedrag? En wat weet de top?
	3.7		**Bespreekbaarheid**. Door over regels te spreken worden gebruikers geholpen bij de interpretatie ervan.Gesignaleerde risico's of privacyschendingen/datalekken kunnen (veilig) worden gemeld en besproken door medewerkers.
	3.8		**Aanspreekbaarheid** Zijn medewerkers en managers aanspreekbaar op hun gedrag? Is er ruimte om kritiek te uiten?
	3.9		**Handhaving**. Belonen/straffen Het privacybeleid en de daaraan gerelateerde processen worden adequaat gehandhaafd

4			Er zijn voldoende organisatorische en technische maatregelen getroffen om de persoonsgegevens te beveiligen.
	4.1		Er is beleid op het gebied van informatiebeveiliging aanwezig
	4.2		Er wordt op basis van ENSIA verantwoording afgelegd over de informatiebeveiliging
	4.3		Er is zicht op informatiebeveiliging bij samenwerkingsverbanden
	4.4		Bij de teams die met de meeste (bijzondere) persoonsgegevens omgaan zijn belangrijke technische en organisatorische maatregelen aanwezig
	4.5		Op elke afdeling is een privacyambassadeur aangewezen, welke de privacygerelateerde vragen en opmerkingen verzamelt en op de hoogte is

			van de wensen en ontwikkelingen binnen de afdeling.
	4.6		Preventieve maatregelen op het individuele niveau worden toegepast
5			Het toezicht op de uitvoering van de verplichte delen van de AVG is adequaat ingericht
		5.1	De Functionaris Gegevensbescherming houdt adequaat toezicht
		5.2	De FG rapporteert periodiek aan de top van de gemeente over relevante situaties en ontwikkelingen met betrekking tot de gegevensbescherming bij de gemeente. De rapportages van de FG krijgen voldoende aandacht en leiden waar nodig tot (verbeter)acties in de lijn.
		5.3	De rapportages van de FG krijgen voldoende aandacht en leiden waar nodig tot (verbeter) acties in de lijn.
		5.4	De gemeenteraad wordt tenminste eenmaal per jaar geïnformeerd over de bevindingen van de FG en de wijze waarop de gemeente daarmee omgaat.
		5.5	De rapporten van de FG worden zoveel als mogelijk openbaar gemaakt.
		5.6	De stand van zaken rondom de gegevensbescherming wordt gedurende het jaar gemonitord in de planning- en controlcyclus. Grotere afwijkingen worden aan de raad gemeld.

Bijlage 2 – Geïnterviewde functionarissen

Onderzoeksfase	Geïnterviewde Functionaris	Datum
Oriënterende Fase	Portefeuillehouder College B&W	02-05-24
	Teamleider Informatievoorziening	02-05-24
	Functionaris voor de Gegevensbescherming	03-06-24
	Chief Information Security Officer	19-06-24
	Privacy Officer	19-06-24
	Functionaris voor de Gegevensbescherming	30-09-24
Uitvoerende Fase	Controller Informatiebeveiliging	08-10-24
	Gemeentesecretaris/directeur	08-10-24
	Strategisch manager (lid MT)	08-10-24
	Teamleider Publiekszaken en Binnensport	08-10-24
	Teamleider Samenleving Sociaal	08-10-24
	Extern adviseur A3PConsultancy	16-10-24
	Informatiespecialist	16-10-24
	Medewerker Backoffice Publiekszaken	16-10-24
	Voorzitter Ondernemingsraad	16-10-24
	Adviseur Veiligheid en Ondermijning	05-11-24
	Consulent Sociaal Domein	05-11-24
	Teamleider Informatievoorziening	05-11-24
	Chief Information Security Officer	05-11-24
	Teamleider Inwoners	13-11-24
Afrondende Fase	Functionaris voor de Gegevensbescherming	15-11-24

Bijlage 3 – Overzicht van geraadpleegde stukken

- Accountantsverslag 2023 Gemeente Nederweert, BDO d.d. 28-06-2024
- Adviesnota afwikkeling datalek dd 6/9/2022 van AVG Juristen
- Algemene Verordening Gegevensbescherming (Verordening (EU) 2016/679 van het Europees Parlement en de Raad d.d. 27-4-2016)
- Anonimiseringsrichtlijn Gemeente Nederweert 2024, versie 1.1 d.d. 30-11-2023
- Autoriteit Persoonsgegevens, AVG Algemeen
- Autoriteit Persoonsgegevens, De AVG in een notendop
- Autoriteit Persoonsgegevens, Gemeenten en privacy: wat kunt u als raadslid doen bij samenwerkingsverbanden, versie 1, oktober 2022
- Autoriteit Persoonsgegevens, Gemeenten en privacy: wat kunt u als raadslid doen versie 2, oktober 2022
- Autoriteit Persoonsgegevens, Handreiking Privacy in een jaarverslag, versie december 2023
- Autoriteit Persoonsgegevens, Praktisch AVG: Data protection impact assessment (DPIA)
- Baseline Informatiebeveiliging Overheid (BIO) Handreiking BIO2-opmaat Versie 2.3 d.d. 23-08-2024
- Baseline Informatiebeveiliging Overheid (BIO) versie 1.04zv d.d. 17-06-2020
- Baseline Informatiebeveiliging Overheid van Digitale Overheid-Cybersecurity (link)
- Begroting gemeente Nederweert 2022
- Begroting gemeente Nederweert 2023
- Begroting gemeente Nederweert 2024
- BIO als hulpmiddel voor privacy, presentatie BIO (link)
- Checklist DPIA, VNG
- De 10 bestuurlijke principes voor informatiebeveiliging Behorende bij de Baseline Informatiebeveiliging Overheid (BIO): VNG januari 2019
- DPIA Jongeren in beeld, MT-23-00412, dd 13-2-2023
- Dreigingsbeeld Informatiebeveiliging 2023 → 2024, Informatie beveiligingsdienst VNG 2022
- ENSIA Notitie Verantwoordingsstelsel 2023 – 2024, VNG Realisatie versie 1.0 d.d. 14-3-2023
- ENSIA toelichting VNG (https://vng.nl/projecten/ensia)
- FG AVG GAP Analyse Nederweert, april 2024
- FG Jaarrapportage Nederweert 2020-2021
- FG jaarverslag Nederweert 2022-2023
- FG jaarverslag Nederweert 2023-2024
- FG, Auditverslag Protocol Ondermijning d.d. 1 november 2021
- Gemeente Nederweert, Klachtenoverzicht 2021
- Gemeente Nederweert, Klachtenoverzicht 2022
- Gemeente Nederweert, Klachtenoverzicht 2023
- Gemeentebreed Informatieveiligheidsbeleid, actualisatie 2018 d.d. februari 2018 (nog geldig v.w.b. ‘tactische onderdelen’)
- Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene

verordening gegevensbescherming, Ministerie van Justitie en Veiligheid, versie 2.0 d.d. 15-04-2023 (link)
- Handreiking 'Stappenplan DPIA' voor gemeenten, Informatiebeveiligingsdiens VNG
- Handreiking BIO voor kleine gemeenten, Informatie beveiligingsdienst VNG versie 1.0 juli 2019
- Handreiking en sjabloon 'Samen naar een kwalitatief goede DPIA', informatiebeveiligingsdienst VNG, versie 1.0 d.d. 6-9-2024
- Handreiking Positionering en taken van de FG, Informatiebeveiligingsdienst VNG, versie 2.2 juni 2020
- Het borgen van de Algemene Verordening Gegevensbescherming in de gemeentelijke organisatie, VNG Realisatie versie, december 2018
- Informatiebeveiliging Governance versie 1.0 d.d. 30-10-2023
- Interne Controleplan 2024 Gemeente Nederweert, d.d. 1-5-2024
- Jaarrekening 2023 Gemeente Nederweert
- KPMG, Acht basis soft controls, februari 2016 (link)
- Landsadvocaat: Review Privacy Protocol Ondermijning Gemeente Nederweert versie 1.4 d.d. 17-1-2024
- Managementletter 2023 Gemeente Nederweert, BDO d.d. 2-2-2024
- Must have DPIA's; lijst met hoog risicoprocessen van VNG/IBD (link)
- Naar een Waardenvolle Informatiesamenleving, Digitale Agenda Gemeenten 2024 (link)
- NBA Handreiking bij Volwassenheidsmodel Informatiebeveiliging (link)
- NBA-handreiking 1148 Het verkrijgen van inzicht in soft controls in het kader van de jaarrekeningcontrole. Impact van cultuur en gedrag op de risicoanalyse, Koninklijke Nederlandse Beroepsorganisatie van Accountants, d.d. 8 februari 2022
- Openbare Besluitenlijst B&W Vergadering 17 maart 2020 – met o.a. goedkeuring diverse onderdelen privacybeleid.
- Organisatieregeling Nederweert 2024 d.d. 13-8-2024, ingaande op 1-9-2024
- Personeelshandboek Gemeente Nederweert 2023
- Presentatie 'Introductie informatiebeveiliging en privacy' voor nieuwe medewerkers
- Presentatie ICT NML Centraal proces beveiligingsincidenten d.d. 2-5-2024
- Presentatie Informatieavond Informatiebeveiliging ICT NML en Team Informatiebeveiliging gemeente Nederweert 23 januari 2023
- Presentatie SIO 2023
- Privacy beleid gemeente Nederweert 2024-2027, Concept versie 0.9
- Privacybeleid gemeente Nederweert 2020 – 2023 versie 0.3 d.d. 04-10-2019
- Privacyprotocol Ondermijning Nederweert 2020 (Besluit van het college van burgemeester en wethouders van de gemeente Nederweert houdende regels omtrent privacy getekend 14-07-2020, geldend m.i.v. 17-07-2020)
- Privacyverklaring Gemeente Nederweert (link)
- Procedure beveiligingsincidenten en datalekken gemeente Nederweert
- Raadsinformatiebrief ENSIA 2023 nr. RIV-24-00842 d.d. 10-4-2024
- Raadsinformatiebrief Register Verwerkingsactiviteiten 2024 B&W nr. RIV-24-00851 d.d. 30-04-2024
- Raadsinformatiebrief Verwerkingsregister 2023 College van B&W RIV-23-00750 d.d. 23 mei 2023

- Raadsinformatiebrief Zelfevaluatie ENSIA 2021 nr. RIV-22-00648 d.d. 15-3-2022
- Rapportage Controles Suwinet 2024 Q1 dd 11-10-2024
- Regeling Toegang tot mailbox of bestanden van medewerkers Versie: 1.1 Datum: 11-05-2023
- Richtlijnen voor het toepassen van algoritmen door overheden en publieksvoorlichting over data-analyses, Ministerie van Justitie en Veiligheid d.d. 1-3-2021
- Sectorbeeld overheid 2024 Autoriteit Persoonsgegevens
- Strategisch Gemeentelijk Informatiebeveiligingsbeleid Nederweert 2023 tot 2024 Gebruikersversie versie 1.0 d.d. 21-08-2023
- Strategisch Gemeentelijk Informatiebeveiligingsbeleid Nederweert 2023 tot 2024 versie 1.0 d.d. 21-08-2023
- Third Party Mededeling ICT NML 2024 door BKBO
- Uitvoeringswet Algemene verordening gegevensbescherming
- Verordening gegevensverstrekking basisregistratie personen Nederweert 2022 d.d. 22-02-2023
- Verwerkersovereenkomst met PLANgroep d.d. 20-7-2018
- Verwerkersovereenkomst uitvoering Dienstverleningsovereenkomst Schulddienstverlening met gemeente Weert d.d. 25-9-2024
- Verwerkingsregister B&W Gemeente Nederweert 2024
- Website Samenwerkingsverband Same Ein (link)
- Werkwijze Bodycam, infographic (link)

Bijlage 4 – Overzicht van mogelijke verbeterpunten

Aard	Mogelijk verbeterpunt	Vindplaats
Urgente verbeterpunten	Delen van het 'interne' privacybeleid zijn strijdig met de AVG.	3.2.2
	Het aantal uitgevoerde DPIA's blijft achter bij wat mag worden verwacht	3.3.2.4
Aandachtspunten	Van het 'externe' privacybeleid staat ook de oude versie nog als geldig online	3.2.2
	Het 'interne' privacybeleid is verlopen en staat als concept versie in JOIN. Aan vervanging wordt gewerkt, maar roept vragen op	
	Het privacybeleid is versnipperd en niet volledig openbaar gemaakt	
	De gemeenteraad is slechts beperkt betrokken geweest bij het privacybeleid	
	Het privacyreglement voor persoonsgegevens van personeelsleden bestaat niet	
	De anonimiseringsrichtlijn beschermt de privacy van medewerkers niet	
	De Ondernemingsraad (OR) is weinig betrokken bij het privacybeleid en de uitvoering	
	De juistheid, volledigheid en relevantie van de bij de verwerkingen opgenomen informatie is wisselend	3.3.2.1
	'Overkoepelende/administratieve' informatie ontbreekt bij het verwerkings-register	
	Het is niet voor iedereen in de organisatie duidelijk wie de FG is en wat zijn taken zijn	3.3.2.2
	De privacyverklaring voldoet aan de meeste, maar niet aan alle daarvoor geldende eisen	3.3.2.3
	De verantwoordelijkheden rondom DPIA's zijn beschreven in het beleid, maar worden in de praktijk niet altijd ingevuld	3.3.2.4
	Het verwerkings-register maakt niet inzichtelijk welke bestaande verwerkingen een hoog privacyrisico opleveren, noch hebben wij elders een dergelijk overzicht gevonden	
	De gemeente heeft een overzicht van verwerkers die in hun opdracht persoonsgegevens verwerken; deze is echter niet in alle gevallen actueel	3.3.2.5
	Er is weinig structureel toezicht op de gemaakte afspraken	
	Er is een datalekregister aanwezig, echter niet alles wordt daarin vastgelegd	3.3.2.6
	Delen van de benodigde procesmatige informatie ontbreekt in het datalekregister	
	De 'knop' op huisnet is niet bij iedereen bekend	3.3.2.7
	Afwegingskaders voor melding aan AP en betrokkenen zijn beschreven, echter incorrect	
	Een crisiscommunicatieplan is niet beschikbaar, maar wordt ook niet nodig geacht	
	Meldingen van (mogelijke) privacyschendingen die als klacht binnenkomen worden niet doorgeleid naar de datalekprocedure	
	Afspraken met de raad over hun betrokkenheid bij datalekken zijn niet gemaakt	
	Procedures voor afhandeling verzoeken rechten betrokkenen slechts beperkt aanwezig en betrokkenen niet adequaat geïnformeerd	3.3.2.10
Aandachtspunten	Het is voor betrokkenen onduidelijk aan welke samenwerkingsverbanden de	3.3.2.12

Aard	Mogelijk verbeterpunt	Vindplaats
(vervolg)	gemeente deelneemt en hoe de afspraken daarbij zijn over het omgaan met persoonsgegevens	
	De behoefte aan opfrissing bij personeel is meermalen benoemd	3.4.2.1
	Het voorbeeldgedrag in de organisatie roept een wisselend beeld op	3.4.2.2
	Werkdruk en druk vanuit college worden gezien als risico voor fouten	3.4.2.4
	Kantoortuin concept met flexplekken biedt voordelen, maar ook risico's	
	Over handhaving bij overtreding van privacyregels bestaat een divers beeld	3.4.2.7
	Het aantal meldingen van incidenten is onrealistisch laag. Het zicht op incidenten is hierdoor in de hele organisatie beperkt	3.4.2.8
	Er is informatiebeveiligingsbeleid. Deze is versnipperd	3.5.2
	Een overkoepelend beeld van de situatie van de informatiebeveiliging ontbreekt. De verantwoording aan de raad over de informatiebeveiliging is incompleet.	
	Op DigiD en Suwinet na, vindt de gehele ENSIA plaats op basis van zelfevaluatie	
	Zicht op informatiebeveiliging bij verwerkers en samenwerkingsverbanden wisselt	
	Vertrouwelijke stukken over informatiebeveiliging waren openbaar	
	Autorisatiebeheer is geregeld, maar kan op onderdelen beter	
	Het stelsel van privacy-ambassadeurs functioneert niet optimaal	
	De bevindingen van de FG worden niet met de raad gedeeld of (op een andere manier) openbaar gemaakt	3.6.2
	Planning, control en verantwoording rondom bescherming persoonsgegevens is mager	