GEMEENTE ENSCHEDE



TOEZICHTSPLAN FUNCTIONARIS GEGEVENS-BESCHERMING 2024

GEMEENTE ENSCHEDE

ENSCHEDE

INHOUDSOPGAVE

INLEIDING 3

LEESWIJZER 3

TAAKINHOUD FG 3

Toezicht houden 3
Adviseren en informeren 4

UITGANGSPUNTEN BIJ PRIVACY TOEZICHT 5

FOCUS FG-TOEZICHT IN 2024 6

TE HANTEREN WERKWIJZE BIJ HET HOUDEN VAN TOEZICHT 8

Algemene AVG-compliance 8
Verwerkingsregister 8
Data Protection Impact Assessments (DPIA's) 9
Uitoefening rechten door betrokkenen 9
Datalekken 9
Bewustwording 10
Transparantie 10
Wet politiegegevens (Wpg) 10
Overig 11

JAARVERSLAG OP BASIS VAN TOEZICHTSPLAN 12

Rapportages 12
Verbetervoorstellen 12

LANGE TERMIJN TOEZICHTSPLAN VANAF 2025 12

INLEIDING

De Functionaris Gegevensbescherming (FG) fungeert als onafhankelijke toezichthouder en adviseur omtrent de naleving van de Algemene Verordening Gegevensbescherming (AVG) en de Wet politiegegevens (Wpg). Tevens dient de FG als contactpunt voor de Autoriteit Persoonsgegevens (AP) en als aanspreekpunt voor betrokkenen (inwoners, medewerkers en andere personen waarvan de gemeente gegevens verwerkt).

Dit document beschrijft hoe de toezichthoudende taak door de FG in 2024 wordt ingevuld. Het doel is om de het college, de raad, de directie en het management te informeren over de werkwijze bij het toezichthouden.

LEESWIJZER

Hieronder volgt eerst een korte beschrijving van de taakinhoud van de FG.
Daarna volgen de uitgangspunten bij het toezicht en de focus voor 2024.
Vervolgens wordt stilgestaan bij het jaarverslag en de daaruit voortvloeiende verbetervoorstellen.
Dit document wordt besloten met een doorkijk naar 2025 en daarna.

TAAKINHOUD FG

De wettelijke taken en bevoegdheden van de FG zijn opgenomen in artikel 39 van de AVG.[1]

TOEZICHT HOUDEN

De FG ziet erop toe dat binnen de gemeente de regels van de AVG en de Wpg worden nageleefd. In het Reglement van de Functionaris Gegevensbescherming is de landelijke regelgeving vertaald naar de gemeentelijke organisatie en geeft de kaders weer voor de wijze waarop de FG van gemeente Enschede de taken en bevoegdheden onafhankelijk en zonder enige belemmering kan uitoefenen. De FG toetst de AVG- en Wpg-compliance in grote lijnen aan de hand van het AVG-borgingsproduct van de VNG[2] en de uitkomsten van de Wpg-audits (intern en extern) die zijn uitgevoerd. De FG houdt ook toezicht op basis van de door de gemeente bijgehouden registers zoals het datalekkenregister en het verwerkingenregister en op basis van informatie die deze krijgt binnen de overleggen waaraan de FG deelneemt of voor uitgenodigd wordt. Daarnaast geeft de FG gevraagd en ongevraagd advies ten aanzien van bijvoorbeeld lopende zaken of ontwikkelingen.

[1] Zie ook het paper van de Autoriteit Persoonsgegevens over de positionering van de FG (https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/positionering_van_de_fg.pdf)
[2] https://www.informatiebeveiligingsdienst.nl/avg-borgingsproduct-3-0/

Bij ad hoc of incident gedreven toezicht vindt onder andere toetsing plaats naar aanleiding van vragen of klachten van betrokkenen of ontwikkelingen binnen de gemeente.

ADVISEREN EN INFORMEREN

De FG adviseert en informeert de verwerkingsverantwoordelijke over haar verplichtingen op grond van de AVG, de Uitvoeringswet AVG, de Wet Politiegegevens en andere privacywetgeving. De FG heeft geen formele bevoegdheid om een bindend advies te geven, maar diens oordeel is ‘zwaarwegend’. Dit betekend dat alleen goed beargumenteerd en gearchiveerd van het advies afgeweken mag worden.

Ten aanzien van de DPIA geeft de AVG aan dat de verwerkingsverantwoordelijk het advies van de FG moet inwinnen (art 35, lid 2 AVG), en dat dit advies, samen met de beslissing van de verwerkingsverantwoordelijke daarover, in de DPIA moet worden vastgelegd èn dat de FG moet toezien op de uitvoering van de DPIA 9 art 39 lid1 onderdeel c AVG). Het is daarom belangrijk dat de organisatie de FG zo vroeg mogelijk betrekt bij de DPIA en om diens advies vraagt. De FG heeft hierin primair een adviserende taak (adviseren over wet- en regelgeving) en is in principe niet betrokken bij het uitvoeren van de DPIA, zodat deze vrij is om te adviseren over de uitkomsten (risico’s) daarvan. De FG ziet ook toe op de uitvoering van dit advies.

Bij een datalek dient de verwerkingsverantwoordelijke de FG te betrekken en toetst de FG het besluit van de verwerkingsverantwoordelijke of een datalek al dan niet gemeld wordt bij de AP en de betrokkene(n). De FG ziet ook toe op de afhandeling. Het doen van een (voorlopige) melding van een datalek is de verantwoordelijkheid van de verwerkingsverantwoordelijke. Daarnaast is de FG bevoegd om als uiterst middel ook zelfstandig een datalek te melden.

De FG adviseert tot slot over technische beveiligingsmaatregelen, maar ook over organisatorische maatregelen. Denk bij dit laatste aan beleid, maar ook aan privacy bewustwording. De FG heeft bij deze maatregelen een aanjagende functie en stimuleert de organisatie. Hieronder vallen activiteiten als werkoverleggen en bezoeken, publiceren van informatie voor medewerkers, adviseren over awareness-tools.

(Artikel 39 bepaalt verder dat de FG contactpunt is voor de toezichthouder. Dat spreekt voor zich en wordt hier verder buiten beschouwing gelaten).

UITGANGSPUNTEN BIJ PRIVACY TOEZICHT

Om het toezicht effectief en doelmatig vorm te geven, worden de volgende uitgangspunten gehanteerd:

Risico gebaseerde aanpak

De AVG en de Wpg hanteren een op risico gebaseerde handelswijze. Daarbij worden de grootste risico's als eerste onderzocht en waar mogelijk gemitigeerd.

Aantoonbaarheid

Het principe van accountability staat centraal in de AVG en Wpg. Dat betekent dat je als organisatie moet kunnen aantonen dat je op de juist wijze omgaat met persoonsgegevens. Inspanningen moet aantoonbaar en – waar mogelijk – meetbaar worden gemaakt. Belangrijke thema's die aantonen dat de gemeente 'in control' is, zijn het verwerkingsregister, het uitvoeren van (pre-) DPIA's, het faciliteren van de rechten van betrokkenen, de afhandeling van datalekken, bewustwordingsactiviteiten onder medewerkers en transparantie.

Focus Autoriteit Persoonsgegevens

De toezichthouder, de AP, heeft voor 2024 in haar jaarplan aangegeven op welke wijze en op welke thema's zij dit jaar gaat toezien.[3] Daarbij heeft zij vijf focusgebieden weergegeven:



Kernpunten uit deze focus zijn verwerkt in het toezichtsplan en zullen teven gehanteerd worden bij het adviseren op onderwerpen die gedurende het komende jaar gaan ontstaan en de revue zullen passeren.
Het onderdeel 'Digitale overheid' wordt hieronder toegelicht. Voor de overige focusgebieden wordt verwezen naar het jaarplan van de AP.

Digitale overheid

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

Wat doen we in ieder geval in 2024?

- We reserveren extra capaciteit om onderzoek te doen naar overheden en uitvoeringsorganisaties die persoonsgegevens van burgers gebruiken in algoritmes.
- We besteden opnieuw aandacht aan het delen van gegevens tussen verschillende onderdelen van de overheid en andere organisaties. Daarnaast geven we aandacht aan de risico's van het gebruik van algoritmes bij de overheid, zoals discriminatie.
- We delen gevraagd en ongevraagd kennis over gegevensuitwisseling in het sociaal domein en over privacywaarborgen bij fraudebeleid en schuldhulpverlening.

[3] https://www.autoriteitpersoonsgegevens.nl/documenten/ap-jaarplan-2024

Actualiteiten

De media besteden steeds meer aandacht aan het onderwerp ‘Privacy’. Het is belangrijk dat het toezicht actuele onderwerpen omvat die op maatschappelijk niveau spelen. Denk daarbij aan het toenemende aantal inzageverzoeken, het koppelen van persoonsgegevens door de overheid, het gebruik van Artificial Intelligence, zoals de toepassing van algoritmen of tools zoals ChatGPT.

FOCUS FG-TOEZICHT IN 2024

Het toezicht wordt in 2024 vormgegeven aan de hand van de volgende onderwerpen:

Onderwerp	Hoe krijgt het toezicht vorm?
Algemene AVG-compliance	De FG gaat na of de AVG-compliance door de organisatie juist wordt beoordeeld en of verbeteracties worden doorgevoerd.
Verwerkingsregister	De FG toetst de volledigheid en actualiteit van het register. Hierbij is ook aandacht nodig voor het actueel houden van het register en het beleggen van de verantwoordelijkheden hiervan bij interne ‘eigenaren’. In 2023 heeft de FG aangegeven dat het register op een aantal onderdelen moet worden aangevuld. Hierbij gaat het om: • het weergeven en in kaart brengen van alle samenwerkingverbanden waarin de gemeenten Enschede deelneemt en de daarbij behorende datastromen. • Gegevens over of een DPIA verplicht is (middels het uitvoeren van een Pré-DPIA) voor betreffende verwerking of de DPIA ook is uitgevoerd en wanneer deze moet worden herzien De FG toetst of deze acties in 2024 inderdaad worden uitgevoerd en geeft waar nodig adviezen tijdens het traject.
DPIA’s	De FG toetst of terecht wordt besloten of een DPIA al dan niet noodzakelijk is (middels de Pré-DPIA-rapportage), bekijkt hoeveel en voor welke verwerkingen DPIA’s zijn uitgevoerd en of adviezen wordt opgevolgd. Ook is aandacht nodig voor de verbindingen die er liggen tussen de uitkomsten van de DPIA en de verwerkersovereenkomst, en de gegevens verkregen uit de DPIA en opname daarvan in het verwerkingenregister. Als laatste, maar wel voorwaardelijk, is dat degenen die met het uitvoeren van een DPIA belast zijn meer kennis krijgen over het proces. In 2023 heeft de organisatie geïnvesteerd in een tweetal incompany trainingen. De FG heeft voor 2024 geadviseerd deze ook in 2024 en daarna te blijven organiseren.
Uitoefening rechten door betrokkenen	De FG controleert of de organisatie de AVG goed toepast en ziet er op toe dat betrokkenen hun privacyrechten kunnen uitoefenen en of de organisatie hen hierin goed faciliteert. De FG heef adviezen gegeven om dit toezicht beter te kunnen vormgeven. De FG vraagt op hoeveel verzoeken zijn gedaan, is beschikbaar voor

	advies bij het behandelen van een verzoek en toetst steekproefsgewijs of deze goed en tijdig zijn afgehandeld.
Datalekken	De FG toetst of op juiste wijze aan de registratie- en meldplicht wordt voldaan, is beschikbaar voor advies bij het behandelen en/of onderzoeken van datalekken en toetst of datalekken juist zijn afgehandeld.
Bewustwording	De FG toetst welke bewustwordingsactiviteiten al dan niet in samenhang worden uitgevoerd. Daarnaast zal de FG samenwerken met de privacy-offers van Gemeente Enschede en de CISO aangaande bewustwordingsactiviteiten zoals scholing, acties, thema-weken enz.
Transparantie	De FG controleert of de gemeente transparant is ten aanzien van haar verwerkingen.
Wpg	De FG houdt toezicht op de implementatie en naleving van de Wpg en adviseert de organisatie daarover. De FG ziet toe of het verbeterplan dat in 2023 is opgesteld (op basis van de aanbevelingen vanuit de externe audit die in december 2022 is uitgevoerd) de juiste aandacht krijgt. De FG ziet toe op de uitvoering van een herbeoordeling op de aandachtspunten uit de externe audit van december 2022 en de tijdige aanlevering hiervan aan de Autoriteit Persoonsgegevens (uiterlijk 1 maart 2024)
Overig	De FG controleert in 2024 of het overzicht van samenwerkingsverbanden waaraan de gemeente deelneemt nog actueel is; dat de nodige informatie over samenwerkingsverbanden wordt opgenomen in het verwerkingenregister en dat verwerkersovereenkomsten actueel zijn.

TE HANTEREN WERKWIJZE BIJ HET HOUDEN VAN TOEZICHT

Hieronder volgt een puntsgewijze toelichting op het bovenstaande schema.

ALGEMENE AVG-COMPLIANCE

Strategische informatiebeveiligings- en privacy beleid

De gemeente Enschede werkt volgens het “Strategisch informatiebeveiligings- en privacy beleid 2021 tot en met 2024”. De gemeente benoemt daarin de uitdaging om optimaal te profiteren van de ontwikkelingen rond digitalisering, maar tegelijkertijd de risico’s van digitalisering te beperken. De missie is een “duurzame en effectieve beveiliging van informatie en bescherming van persoonsgegevens binnen de gemeente.” De gemeente heeft op basis daarvan een aantal speerpunten benoemd, waaronder het centraal zetten van betrokkenen en belanghebbenden en het verankeren van privacy en informatiebeveiliging in op alle niveaus in de organisatie.
Om de goede omgang met persoonsgegevens te toetsen wordt het AVG borgingsproduct 3.0 van de VNG/IBD ingezet en worden afspraken gemaakt over de verplichte audits in het kader van de Wpg.

VERWERKINGSREGISTER

Het is belangrijk om een goed overzicht te hebben van alle gegevensverwerkingen die plaats vinden. Hiervoor dient het benodigde verwerkingsregister actueel en compleet te zijn. Dit overzicht is nodig om de belangrijke risico’s in beeld te hebben, maar ook voor het uitoefenen van privacy rechten door betrokkenen. In dit verwerkingsregister wordt ook het doel van, en de wettelijke grondslag voor, de verwerking van deze gegevens vastgelegd. Het is dus een belangrijk document om aan te tonen dat de gemeente voldoet aan één van de belangrijkste beginsel van de AVG voldoet (verantwoordingsplicht).

Onder regie van de Privacy Officers is het verwerkingsregister in 2022 overgezet naar een nieuwe applicatie (I-navigator) en het register is daarna geactualiseerd. Daarna is een procedure geschreven om het register actueel te houden en waarbij de verantwoordelijkheid wordt belegd in de lijn (waar deze verantwoordelijkheid hoort). Op dit moment ontbreken nog een aantal zaken in het register. Samenwerkingsverbanden zijn nog niet opgenomen in het verwerkingenregister en het register mist informatie over of de verwerkingen die zijn opgenomen in het verwerkingenregister:

- Verwerkingen zijn waarbij het verplicht is om een DPIA voor uit te voeren;
- Of een DPIA ook daadwerkelijk is uitgevoerd;
- Wanneer deze is uitgevoerd en of deze is voorzien van een advies van de FG;
- Wanneer deze uiterlijk moet worden herzien.

Hiervoor is het nodig om een scan op al deze processen uit te voeren op basis van informatie die bij verschillende domeinen en vakgroepen al dan niet aanwezig is. De FG heeft geadviseerd om deze in 2024 uit te voeren.

➔ *De FG toetst de volledigheid en actualiteit van het register. Daarnaast toetst de FG of de procedure om het register actueel te houden, is geïmplementeerd en wordt gehanteerd in de organisatie. De FG controleert of de nodige aanvullingen in het register worden uitgevoerd.*

➔ *De FG zal steekproefsgewijs de rechtmatigheid van een aantal gevoelige verwerkingen in het register toetsen op basis van de vereisten in de AVG.*

DATA PROTECTION IMPACT ASSESSMENTS (DPIA'S)

Onder de AVG moeten voor gevoelige verwerkingen zogeheten Data Protection Impact Assessments (DPIA's) worden uitgevoerd. De AP heeft dit voor een vast aantal verwerkingen verplicht gesteld en daarnaast geldt dat bij voorgenomen en bestaande verwerkingen aan de hand van een aantal criteria getoetst moet worden of een DPIA al dan niet noodzakelijk is. Een DPIA is een risicoanalyse waarbij privacy risico's van (voorgenomen) gegevensverwerkingen in kaart worden gebracht én risico's worden verkleind.

➔ *De FG toetst of binnen de organisatie bekend is wanneer een DPIA uitgevoerd dient te worden en of de juiste afwegingen worden gemaakt rondom de noodzaak tot het uitvoeren van een DPIA.*
➔ *Ook wordt getoetst waar de verantwoordelijkheid is belegd om een DPIA uit te voeren en of hierbij voldoende kennis aanwezig is om een DPIA op de juiste wijze te kunnen uitvoeren.*
➔ *Daarnaast bekijkt de FG hoeveel en voor welke verwerkingen DPIA's zijn uitgevoerd of DPIA's ter beoordeling worden voorgelegd aan de FG om diens (wettelijk verplichte) advies in te winnen.*
➔ *De FG gaat na in hoeverre gegeven adviezen zijn/worden opgevolgd om risico's te verkleinen.*

UITOEFENING RECHTEN DOOR BETROKKENEN

Onder de AVG hebben mensen van wie de gemeente persoonsgegevens verwerkt een aantal verschillende privacy rechten. Denk aan het recht op inzage of het recht op verwijdering van gegevens. De gemeente dient op tijd en op de juiste manier op deze AVG-verzoeken te reageren. De FG heeft hierin in 2023 een aantal adviezen gegeven om het proces rond het faciliteren van betrokkenen in het uitoefenen van hun rechten beter gestroomlijnd en geborgd kan worden. Het college heeft op basis hiervan een aantal acties uitgezet.

➔ *De FG ziet er op toe dat betrokkenen in staat worden gesteld hun AVG-rechten uit te oefenen. De FG toetst of dit tijdig gebeurt en of de juiste afwegingen zijn gemaakt bij het toekennen of afwijzen van een verzoek. Daarnaast is de FG beschikbaar voor ad hoc advies bij lopende verzoeken.*
➔ *De FG gaat na of de acties die in 2024 zullen worden opgepakt ook daadwerkelijk worden uitgevoerd en tot het beoogde resultaat leiden. Hieronder vallen onder andere de afspraken rond het aanstellen van een AVG-coördinator, het mogelijk maken voor betrokkenen om digitaal via de website een AVG-verzoek te kunnen indienen en het inrichten van een proces voor zakelijk archiveren van AVG-verzoeken.*

DATALEKKEN

Datalekken komen in iedere organisatie voor. Een organisatie waar geen datelekken voorkomen is een utopie. Waar mensen werken worden immers fouten gemaakt. Het is belangrijk dat medewerkers datalekken herkennen en melden. De gemeente moet deze registreren, beoordelen en mogelijk melden aan de toezichthouder en/of betrokkenen.

➔ *De FG toetst het beleid en/of de procedure rondom het melden en afhandelen van datalekken.*
➔ *Daarnaast toetst de FG of op juiste wijze aan de registratie- en meldplicht wordt voldaan. Met andere woorden: worden de datalekken tijdig en op de juiste manier afgehandeld.*
➔ *Verder bekijkt de FG steekproefsgewijs of lering wordt getrokken uit de onderzochte datalekken.*
➔ *De FG is altijd beschikbaar voor ad hoc advies bij het behandelen of onderzoeken van een datalek.*

BEWUSTWORDING

De meeste datalekken worden veroorzaakt door menselijk handelen. Door aandacht te besteden aan bewustwording op het gebied van privacy (en informatiebeveiliging) maak je alle medewerkers weerbaar en verminder je het aantal datalekken. Ook worden andere privacy risico's beperkt wanneer medewerkers bewust zijn.

- ➔ *De FG toetst welke bewustwordingsactiviteiten al dan niet in samenhang worden uitgevoerd en gaat na of de deelname en effectiviteit van de activiteiten wordt gemeten.*
- ➔ *De FG doet aanbevelingen ten aanzien van onderwerpen waarop meer bewustwording of scholing nodig is. Hierbij kunnen de adviezen ook betrekking hebben op specifieke domeinen of bepaalde organisatieniveaus.*

TRANSPARANTIE

Eén van de beginselen van de AVG is dat persoonsgegevens moeten worden verwerkt op een wijze die transparant is voor de betrokkene. Transparantie houdt in dat het voor de betrokkene, zoals inwoners en werknemers, duidelijk is dat zijn of haar persoonsgegevens worden verzameld, gebruikt, geraadpleegd of op een andere manier verwerkt worden en waarom de gemeente dit doet en hoe.

- ➔ *De FG controleert of de gemeente transparant is ten aanzien van haar verwerkingen. Hiervoor wordt onderzocht welke informatie publiekelijk beschikbaar wordt gesteld, zoals een privacy beleid en/of privacy statement.*
- ➔ *De FG controleert of de geboden informatie ook duidelijke informatie is*

WET POLITIEGEGEVENS (WPG)

Bij de uitvoering van wettelijke opsporingstaken door Boa's wordt op de privacy van burgers ingegrepen. De Wet politiegegevens (Wpg) stelt daarom eisen aan de verwerking van politiegegevens. Publieke organisaties die boa's in dienst hebben moeten jaarlijks een interne Wpg-audit uitvoeren. Daarnaast moet om de vier jaar een externe audit worden uitgevoerd.

- ➔ *De FG houdt toezicht op de uitvoering van de aanbevelingen in de rapportage die eind 2022 is aangeleverd naar aanleiding van de externe audit.*
- ➔ *De FG houdt toezicht op de uitvoering van het verbeterplan dat op basis van de aanbevelingen uit de externe audit rapportage is opgesteld.*
- ➔ *De FG houdt toezicht op de naleving van het Wpg-beleid dat in 2023 is opgesteld.*

De taken van de functionaris gegevensbescherming (artikel 36 van de Wet politiegegevens) aangaande de Wpg kunnen als volgt worden samengevat:
De functionaris gegevensbescherming voert periodiek controles uit op het naleven van de wettelijke verplichtingen die voortkomen uit de Wpg, waaronder de controle op:

1. het hebben van een beleid aangaande de uitvoering van de Wpg;
2. de bewustwordingsverplichting;
3. het autorisatieproces met betrekking tot het vastleggen van politiegegevens ;
4. de kwaliteit en waarborging van de juistheid van de nauwkeurigheid van politiegegevens;
5. het verwerken van politiegegevens;

6. de bewaartermijnen;
7. het ter beschikking stellen en verstrekken van politiegegevens;
8. de controle op de informatiebeveiliging en de controle op het uitvoeren van een risicoanalyse;
9. het register voor verwerkingen;
10. de verplichtingen ten aanzien van de audit;
11. De functionaris gegevensbescherming stelt periodiek rapportages op en rapporteert zo nodig rechtstreeks aan de gemeente [hierover moeten nog aanvullende afspraken gemaakt worden: aan wie en wanneer].

OVERIG

Naast voornoemde speerpunten richt het toezicht in 2024 zich nog op twee andere aandachtsgebieden. Het gaat daarbij om samenwerkingsverbanden en databeveiliging.

SAMENWERKINGSVERBANDEN

De titel van het jaarplan van de AP is: “Beschermen van burgers in een digitale wereld’ Zij verwacht daarbij dat overheidsorganisaties terughoudend zijn met het delen van gegevens. Zij geeft hierbij aan; “Zonder de bescherming van ons grondrecht op gegevensbescherming kunnen andere grondrechten in gevaar komen. Zoals het recht op privacy en het recht om niet gediscrimineerd te worden” Het is aan overheidsbestuurders en aan de wetgever om een goede afweging te maken over het nut en de noodzaak van het gebruik van data en nieuwe verwerkingen.[4] Hierbij staat doelbinding voorop; de gegevens mogen niet voor een ander doel worden gebruikt, dan waarvoor ze zijn verkregen. De gemeente neemt deel aan veel samenwerkingsverbanden waarin veel gegevens worden gedeeld.

- ➔ *De FG controleert in 2024 of het overzicht van samenwerkingsverbanden nog actueel is en of met al onze samenwerkingspartners de benodigde overeenkomsten in het kader met uitwisseling van gegevens zijn afgesloten*
- ➔ *De FG controleert in 2024 of de informatie over samenwerkingsverbanden (op de juiste wijze) is opgenomen in het verwerkingenregister*
- ➔ *De FG adviseert de organisatie waar nodig over veilige gegevensuitwisseling binnen deze samenwerkingsverbanden en is beschikbaar voor aanvullend advies waar nodig.*
- ➔ *De FG is graag betrokken in het kader van privacy by design indien samenwerkingsverbanden worden herzien of nieuw opgezet.*

DATABEVEILIGING

De AP controleert overheidsorganisaties op hun beveiligingsniveau en stimuleert om werk te maken van een sterke IT- en datahuishouding. Privacy-risicomanagement en audits van IT-systemen worden gezien als onderdeel van de databoekhouding.[5] De gemeente geeft haar informatiebeveiliging vorm aan de hand van o.a. de Baseline Informatiebeveiliging Overheid (BIO). De gemeente verantwoordt zich over de staat van informatiebeveiliging aan de hand van het ENSIA-kader. De FG wordt hierbij actief betrokken. Voor een verantwoording en het toezicht op databeveiliging wordt verwezen naar de Chief Information Security Officer (CISO).

[4] AP jaarplan 2024 https://www.autoriteitpersoonsgegevens.nl/documenten/ap-jaarplan-2024
[5] Focus AP 2020-2023, Dataprotectie in een digitale samenleving, p. 23.

JAARVERSLAG OP BASIS VAN TOEZICHTSPLAN

Op basis van dit toezichtsplan doet de FG verslag over de privacy compliance van de gemeente. Een dergelijk verslag is niet verplicht vanuit de AVG, is wel een verplichting vanuit de Wpg. De input van het jaarverslag is de AVG-compliance zoals aangegeven vanuit borgingsproduct (uitgevoerd door de Privacy Officers), de externe herbeoordeling op basis van de aandachtspunten uit de externe audit van eind 2022 en de interne audit ten aanzien van de Wpg en een steekproefsgewijs onderzoek/toetsing door de FG. Dit jaar verslag wordt in 2025 aangeboden aan het college en de gemeenteraad.

RAPPORTAGES

De FG brengt periodiek of indien nodig rechtstreeks verslag uit aan de hoogst leidinggevende. Dit kan dus zijn aan de gemeentesecretaris, het college van B&W, de portefeuillehouder gegevensbescherming in het college van B&W, de burgemeester, of de gemeenteraad. Dit verslag is vormvrij dus kan zowel digitaal als mondeling zijn.

VERBETERVOORSTELLEN

De FG zal ten aanzien van het gehouden toezicht op basis van zijn of haar bevindingen verbetervoorstellen opstellen. Hierdoor kan de gemeentelijke organisatie haar risico's beperken.
Daarnaast kan de FG gevraagd of ongevraagd adviezen geven op basis van bijvoorbeeld geconstateerde risico's.

LANGE TERMIJN TOEZICHTSPLAN VANAF 2025

In dit toezichtsplan is een focus gelegd op bepaalde onderwerpen. Het maken van een dergelijke keuze is altijd gebaseerd op een inschatting van wat belangrijk is, die vooraf, aan het begin van het jaar, wordt gedaan. Dat kan er toe leiden dat gedurende het jaar de actualiteit maakt dat keuzes bijgesteld moeten worden, of dat de focus op basis van de actualiteit moet worden verlegd. Ook kunnen keuzes, zowel vooraf als gedurende het jaar er toe leiden dat andere onderwerpen wellicht minder aandacht krijgen.

Daarnaast zou de FG 2024 graag gebruiken om 'de stip op de horizon' verder uit te werken. Toezicht is een complex geheel dat uit veel aspecten bestaat. Denk aan en toezien op:

- Beleid: is het er, is het bekend, werkt het?
- Processen: zijn deze voorhanden en zijn deze helder beschreven?
- Organisatorische inbedding: hoe werkt het in de praktijk?
- Het actief en passief informeren van betrokkenen t.a.v. hun rechten;
- Samenwerken met (mede-) organisaties ;
- Beveiliging van persoonsgegevens (samen met de CISO);
- Verantwoording: hoe de organisatie zelf aantoonbaar kan maken dat deze voldoet aan de AVG en Wpg.

Hoe kan de organisatie hierin transparanter maken waar deze staat? En kan het toezicht hier cyclisch in worden ingericht, zodat de PDCA (hulpmiddel voor kwaliteitsmanagement) hierin rond komt? Met het nog beter leren

kennen van de organisatie wil de FG hier gedurende het jaar informatie over verzamelen om hier in het volgende jaarplan aanbevelingen in te gaan doen.

GEMEENTE ENSCHEDE



Teksten FG, concernstaf.

Datum 16-02-2023

Aan dit document kunnen geen rechten worden ontleend

ENSCHEDE