GEMEENTE ENSCHEDE

JAARVERSLAG FUNCTIONARIS GEGEVENS-BESCHERMING 2023

GEMEENTE ENSCHEDE

ENSCHEDE

INHOUDSOPGAVE

SAMENVATTING

Als onafhankelijk toezichthouder van de gemeente constateert de Functionaris Gegevensbescherming (FG) dat de gemeente Enschede vorderingen maakt wanneer het gaat om het voldoen aan de Algemene Verordening Gegevensbescherming (AVG).
Na de invoering van de AVG in 2018 is de gemeente zich stap voor stap aan het door ontwikkelen tot een organisatie waarbij de bescherming van de aan de gemeente toevertrouwde persoonsgegevens meer en meer ‘in control’ is. Daarnaast zijn diverse professionaliseringsslagen gemaakt of in ontwikkeling. Hierbij een korte samenvatting van wat in de rest van het verslag verder wordt uitgewerkt.

WAT DE GEMEENTE IN 2023 HEEFT BEREIKT:

a. Het college heeft het Reglement voor de Functionaris Gegevensbescherming vastgesteld. In dit reglement is de landelijke regelgeving vertaald naar de gemeentelijke organisatie geeft de kaders weer voor de wijze waarop de FG van de gemeente de taken en bevoegdheden onafhankelijk en zonder enige belemmering kan uitoefenen;
b. In de zomernota heeft het College financiële ruimte gecreëerd voor de aanstelling van een AVG-coördinator om de rechten van betrokkenen beter te kunnen faciliteren. Denk hierbij aan AVG-verzoeken zoals (concernbrede) inzageverzoeken of verwijderingsverzoeken;
c. In de zomernota heeft het College financiële ruimte gecreëerd voor een capaciteitsuitbreiding voor de privacy officers waarbij binnenkort ieder domein over een eigen privacy officer kan beschikken;
d. Het verwerkingenregister is geactualiseerd en gedigitaliseerd en de publieksvriendelijke versie is gepubliceerd op de internetpagina van de gemeente. Daarnaast is een procedure opgesteld om het register actueel te kunnen houden;
e. Er is een nieuwe procedure voor het uitvoeren van een Data Protection Impact Assessment (DPIA)vastgesteld. Een DPIA uitvoeren is bepaalde situaties wettelijk verplicht, bijvoorbeeld wanneer sprake is van hoog risicoverwerkingen. Bij de procedure zijn ook heldere formats en gebruikershandleidingen beschikbaar die de uitvoerder behulpzaam zijn bij het goed uitvoeren van deze risicoanalyse. Daarnaast is geïnvesteerd in de kennis van ambtenaren door een DPIA-training aan te bieden;
f. Er is een verbeterplan opgesteld om beter te kunnen voldoen aan de Wet Politiegegevens (Wpg), er is een Wpg beleid opgesteld en een hercontrole uitgevoerd op de nog openstaande punten die zijn benoemd in de externe audit van december 2022;
g. De datalekkenprocedure is herzien.

WAAR IN 2023 ACTIES IN ZIJN UITGEZET EN IN 2024 VERDER VORM KRIJGEN:

a. Zaakgerichte archivering van uitgevoerde DPIA’s;
b. Zaakgerichte archivering van AVG-verzoeken;
c. Het mogelijk maken om een AVG-verzoek te doen via een digitaal formulier op de website van gemeente Enschede;

d. Actualisering van de informatie over privacy en privacy-gerelateerde onderwerpen op de website van de gemeente Enschede;
e. Aanbestedingstraject voor een nieuwe aanbieder van awareness trainingen rond privacy en informatieveiligheid;
f. In de nieuwe datalekkenprocedure is opgenomen dat de datalekken vanaf 1 maart a.s. worden afgehandeld door de privacy officers (nu nog door het securityteam). Voordeel is dat hierbij het leren van datalekken beter kan worden vormgegeven. De technische aspecten van een datalek worden als voorheen afgehandeld door het securityteam. Datalekken kunnen in de nieuwe procedure 24/7 uniform gemeld worden door zowel in- als externen door inzet van een gestandaardiseerd webformulier.

INLEIDING

Met het jaarverslag van de Functionaris Gegevensbescherming (FG) van de gemeente Enschede wordt beoogd verantwoording af te leggen van de taak van de FG zoals vastgelegd in de Algemene Verordening Gegevensbescherming (art. 39 AVG) en daarmee een beeld te scheppen over waar de gemeente Enschede staat wanneer het gaat om het verwerken van persoonsgegevens conform de AVG. De belangrijkste taak van de FG is dat deze onafhankelijk toezicht en controle houdt op de toepassing en naleving van de Algemene verordening gegevensbescherming en de Wet politiegegevens door de gemeente als organisatie. Binnen de gemeente Enschede zijn deze taken vastgelegd in het FG Reglement. Dit reglement is op 29 maart vastgesteld door het College van Burgemeester en Wethouders en op 15 mei vastgesteld in de gemeenteraad. Daarna is deze op 27 mei is gepubliceerd in het gemeenteblad en op overheid.nl/ Lokale wet- en regelgeving.

Dit jaar verslag gaat in op het algemene beeld van de compliance ten aanzien van de AVG, de bevindingen over het jaar 2023 en de aandachtspunten voor 2024. In het voorjaar van 2023 is afgesproken dat dit verslag jaarlijks zal worden opgesteld en aangeboden aan het college van Burgermeester en wethouders omdat zij eindverantwoordelijk is voor de verwerking van persoonsgegevens. Het college dient kennis te nemen van het jaarverslag en kan uitspraak doen over de vermelde aandachtpunten voor 2024. Daarna kan het college het jaarverslag ter informatie aanbieden aan de gemeenteraad en publiceren op de website van de gemeente. Het jaarverslag wordt tevens aangeboden aan de Gemeentesecretaris en aan de Concerndirectie aangezien zij inhoudelijk verantwoordelijk zijn voor de verwerking van persoonsgegevens binnen de gemeentelijke organisatie.

LEESWIJZER

Deze jaarrapportage bestaat uit twee onderdelen:

In het eerste deel wordt teruggekeken naar het jaar 2023. Wat heeft de gemeente bereikt op het gebied van gegevensbescherming? Welke maatregelen zijn er genomen om te voldoen aan de AVG?
In het tweede deel worden aanbevelingen gedaan om gegevensbescherming en privacy in het jaar 2024 naar een hoger niveau te tillen. Hierbij wordt waar nodig tevens aandacht geschonken aan de technische en organisatorische middelen die nodig zijn om dit hogere niveau te bereiken.

In het toezichtsplan voor 2023 zijn de volgende aandachtsgebieden aangemerkt:

1. Algemene AVG-compliance
2. Verwerkingsregister
3. DPIA's
4. Uitoefening rechten door betrokkenen
5. Datalekken
6. Bewustwording
7. Transparantie
8. Wpg
9. Overig

De terugblik op 2023 vindt plaats aan de hand van deze aandachtsgebieden. Het eerste aandachtsgebied, de algehele AVG-compliance neemt daarbij een bijzondere plaats in.

De algehele AVG-compliance[1] wordt in de gemeente Enschede gemeten aan de hand van het IBD AVG-borgingsproduct. In dit product worden zeven thema's onderscheiden, te weten:

- Beleid
- Processen
- Organisatorische inbedding
- Rechten van betrokkenen
- Samenwerking
- Gegevensbescherming
- Verantwoording

Enkele van deze onderwerpen komen ook terug in de andere focusgebieden. Om overlap te voorkomen wordt daarbij zoveel mogelijk terugverwezen.

[1] Hiermee wordt bedoeld dat binnen de gemeente aan de hand van het AVG Borgingsproduct wordt gemeten in hoeverre de gemeente voldoet aan de eisen die voortvloeien uit de AVG. Daarbij moet worden opgemerkt dat compliance een continu proces is en blijft (en geen 'afvinklijst').

DEEL 1. TERUGBLIK OP 2023

Het jaar 2023 stond in het teken van het verder ontwikkelen van het ‘privacy-team en’ het verder professionaliseren van de gegevensbescherming op basis van het vastgestelde strategische Informatieveiligheid en privacy beleid. In dit beleid staat: "Wij (gemeente Enschede) zijn transparant over de verwerking van persoonsgegevens en staan voor een veilige & rechtmatige verwerking daarvan." Onder het ‘privacyteam’ wordt verstaan: de privacy officers (PO), de Chief Information & Security Officer (CISO) en de Functionaris Gegevensbescherming (FG). De FG hierbij met name FG in haar rol als onafhankelijk toezichthouder en adviseur.

De vorige vaste FG is eind 2021 na een aantal jaren vertrokken en de medewerker die de positie van centrale privacy adviseur heeft vervuld, is medio 2021 van functie gewisseld. Tegenover het vertrek van deze twee functionarissen staat de aanstelling van een drietal decentrale privacy officers in Enschede (geen volledige fte’s). Er was in de periode van 1 december 2021 tot en met 30 november 2022 een interim FG aangesteld. Vanaf 1 december 2022 is weer een vast FG benoemd.
Deze gezamenlijke groep privacy specialisten heeft samen met de CISO gezocht naar een nieuw evenwicht en de juiste verdeling van rollen en taken. Dit is in 2022 in gang gezet maar was nog niet helemaal uitgekristalliseerd. De nieuwe FG heeft daarom in het voorjaar van 2023 een tweetal strategiedagen georganiseerd met de volgende doelen:

- Helderheid krijgen van ieders taken, verantwoordelijkheden en bevoegdheden;
- Nagaan hoe op basis daarvan het beste kan worden samengewerkt om hierbij de organisatie zo goed mogelijk te helpen in het realiseren van haar AVG-compliancy;
- Inzichtelijk maken wat daarbij nodig is vanuit de organisatie om dat te realiseren, in de vorm van capaciteit, kennis en middelen.

Op basis van de uitkomsten van deze strategiedagen zijn gesprekken met het management gevoerd en is in de zomernota van 2023 financiering gevonden voor het aantrekken van een AVG-coördinator en een uitbreiding van de capaciteit van de privacy officers. Hierdoor is binnen ieder domein een privacy officer beschikbaar om de vakgroepen te helpen te voldoen aan de AVG. Deze investering levert de gemeente Enschede het volgende op:

- Meer vertrouwen van de inwoner ten aanzien van hoe de gemeente met hun persoonsgegevens omgaat;
- Privacybescherming door ambtenaren op basis van een natuurlijke en zorgvuldige werkwijze;
- Bewust en effectief datagebruik;
- Een transparante en lerende organisatie kunnen zijn;
- Helderheid over taken, verantwoordelijkheden en verwachtingen;
- Voorkomen van fouten en het voorkomen van boetes en/of herstelkosten;
- Beter vormgegeven van risicomanagement inzake AVG;
- Beter voorbereid zijn op toekomstige ontwikkelingen en nieuwe of wijzigende wet- en regelgeving.

De FG heeft voor 2023 een toezichtplan opgesteld. Deze diende tevens als gespreksleidraad tijdens de kwartaaloverleggen van de FG met de verantwoordelijk wethouder en de gemeentesecretaris.

1. ALGEMENE AVG-COMPLIANCE VOLGENS IBD BORGINGSPRODUCT

BELEID

Het privacybeleid is een kader waarin de gemeente aangeeft aan welke principes zij zich houdt bij de verwerking van persoonsgegevens. Het laat zien hoe de gemeente omgaat met persoonsgegevens en welke maatregelen zij treft om te voldoen aan de relevante wet- en regelgeving.

In 2022 is door de CISO het Strategisch Informatiebeveiliging en privacybeleid opgesteld. Het college in Enschede heeft op 27-09-2022 het 'Strategisch informatiebeveiligings- en privacybeleid' vastgesteld.

Net als in voorgaande jaren zijn metingen uitgevoerd op basis van het IBD AVG Borgingsproduct. Er is een meting uitgevoerd op het Sociaal Domein (inclusief de wijkteams), De DCW en een meting naar de overige domeinen. Deze metingen zijn uitgevoerd met behulp van de nieuwe versie (3.0) van het Borgingsproduct[2].

JAARPLAN2023

Net als in 2022 is op basis van het beleid en de metingen een Jaarplan informatiebeveiliging en privacy 2023 opgesteld (hierna: jaarplan). Dit plan is vastgesteld door de CIO. Een deel van dit jaarplan, voor zover deze betrekking hebben op privacy, is hieronder weergegeven met daarbij de status aan het einde van 2023

Verantwoordelijkheden (governance)
Bij een goede informatiebeveiligings- en privacyorganisatie is het randvoorwaardelijk om taken, rollen en verantwoordelijkheden te beleggen en te borgen in de organisatie, alsmede het hebben van duidelijk beleid en procedures en het weken conform deze kaders.

	Beleid en procedures	Vakgebied	Status
	Opstellen van beleid en procedure voor Privacy by design	Privacy	Doorgeschoven naar 2024
	Opstellen procedure rechten van betrokkene	Privacy	In uitvoering
	Opstellen procedure afhandeling datalekken	Privacy	Afgerond
	Opstellen procedure en format voor uitvoeren DPIA	Privacy	Afgerond
	Opstellen procedure voor anonimiseren (onderdeel van project)	Privacy	Afgerond
	Opstellen procedure voor afhandeling AVG-klachten	Privacy	Doorgeschoven naar 2024
	Opstellen procedure voor actueel houden verwerkingsregister (onderdeel van project)	Privacy	Afgerond
	Opstellen privacy verklaring op de website[3]	Privacy	In uitvoering

Versterken en door ontwikkelen van informatiebeveiliging en privacy (risk)
Door de basisbeveiliging te verhogen en risico's te mitigeren zijn we minder kwetsbaar. Deze projecten en activiteiten dragen bij aan een veilige informatievoorziening en verwerking van persoonsgegevens.

[2] De uitkomsten van de metingen hebben geleid tot discussie over (onder andere) de systematiek en wijze van beoordeling. De beoordeling laat immers ruimte over voor eigen afwegingen (subjectiviteit). Daarnaast is de beoordeling niet helemaal in lijn met de uitkomsten van voorgaande jaren. Het volwassenheidsniveau is niet voor alle organisatieonderdelen gemeten en zou een vertekend beeld geven.

[3] Niet alleen de privacyverklaring maar alle informatie op de website wordt aangepast om zo meer informatie te geven over hoe de gemeente omgaat met privacy en persoonsgegevens.

Projecten	Vakgebied	Status
Toepassen van security en privacy by design in projecten	Privacy & security	Continu proces
Implementeren anonimiseringssoftware	Privacy	Afgerond
Implementeren ISMS voor privacy en verdere uitrol ISMS voor security	Privacy	Gestart
Afronden van project actualisatie verwerkingsregister	Privacy	Afgerond
In beeld brengen van alle samenwerkingen en uitbestedingen	Privacy	Doorgeschoven naar 2024
Herzien bewustwordingscampagne	Privacy & security	In uitvoering
Reguliere werkzaamheden	**Vakgebied**	**Status**
Uitvoeren bewustwordingsactiviteiten	Privacy & security	Continu proces

Naleving (compliance)
Voor de informatiebeveiliging en privacy geldt dat we in overeenstemming met de verplichte en wettelijke kaders, zoals de BIO, AVG en WPG moeten werken. Deze werkzaamheden dragen bij aan de verantwoording en rapportage daarover.

Compliance metingen	Vakgebied	Status
Uitvoeren AVG compliance meting (AVG borgingsproduct in ISMS)[4]	Privacy	Nog niet gepland
Audits	**Vakgebied**	**Status**
Audit Wpg	Business	Uitgevoerd
Reguliere werkzaamheden	**Vakgebied**	**Status**
Bijhouden verwerkingsregister	Privacy	Continu proces
Afhandelen AVG klachten	Privacy	Continu proces
Rapportage	**Vakgebied**	**Status**
Opstellen rapportage beveiligingsincidenten en datalekken	Privacy & security	Afgerond

Naast het actualiseren van het beleid (gerealiseerd), zijn de Wpg-audit (zie blz. 19), het actualiseren van het verwerkingsregister, het herzien van de procedure van rechten van betrokkenen en het actualiseren van de afhandeling van datalekken en het herzien van de DPIA-procedure als belangrijkste acties op het vlak van privacy opgenomen. Samen met de beveiligingsadviseurs is het nieuwe ISMS uitgerold en is gestart met het herzien van de bewustwordingscampagne.

PROCESSEN

De verwerkingen van persoonsgegevens van de gemeente dienen te voldoen aan de AVG. Dit houdt in dat de werkprocessen die persoonsgegevens bevatten getoetst en ingericht moeten worden volgens de volgende beginselen: behoorlijkheid, transparantie, doelbinding, dataminimalisatie, opslagbeperking, juistheid, integriteit en vertrouwelijkheid. Daarnaast kan de gemeente in gevallen verplicht zijn om een

[4] De AVG-compliance metingen worden wel uitgevoerd maar nog niet in alle organisatieonderdelen. En het AVG borgingsproduct is nog niet gedigitaliseerd in het ISMS-systeem.

gegevensbeschermingseffectbeoordeling (Data Protection Impact Assessment, ofwel DPIA[5]) uit te voeren. De FG heeft adviezen gegeven hoe dit proces beter in te richten en te borgen. Aan deze adviezen is opvolging gegeven en in dit verslag wordt daar later verder op ingegaan.

Binnen de gemeentelijke organisatie zijn veel verschillende werkprocessen te onderscheiden.
Belangrijke processen op het gebied van privacy, zoals het de afhandeling van datalekken en de uitoefening van rechten van betrokkenen zijn in 2022 kritisch bekeken. De procedure afhandeling datalekken is op basis van deze inpunt in 2023 aangepast.
De procedure ten aanzien van de rechten van betrokkenen wordt op moment van schrijven geactualiseerd. Hier was meer tijd voor nodig, omdat zowel de wijze waarop betrokkenen een AVG-verzoek kunnen indienen, de wijze waarop hun identiteit kan worden gecontroleerd, de wijze waarop een inzageverzoek kan worden beoordeeld en afgehandeld en de archivering van verzoeken moest worden heroverwogen. Daarnaast waren concern brede inzageverzoeken moeilijk af te handelen onder begeleiding van een binnen een domein gepositioneerde privacy officer en was ook de capaciteit aan privacy officers een beperkende factor. Doordat nu financiële middelen beschikbaar zijn voor de aanstelling van een AVG-coördinator kunnen hier mooie stappen in worden gerealiseerd.

Het streven is om volgend kalenderjaar een aantal andere kritische processen, binnen de domeinen waar veel (bijzondere of gevoelige persoonsgegevens worden verwerkt, aan een steekproef te onderwerpen en te analyseren.

Het DPIA-proces is met en door de privacy officers, CISO op basis van de aanbevelingen van de FG aan de organisatie opnieuw besproken en uitgewerkt, zodat gemeente breed uniform wordt gewerkt. Bij punt 3. DPIA's verderop in dit verslag wordt hier verder op ingegaan.

ORGANISATORISCHE INBEDDING

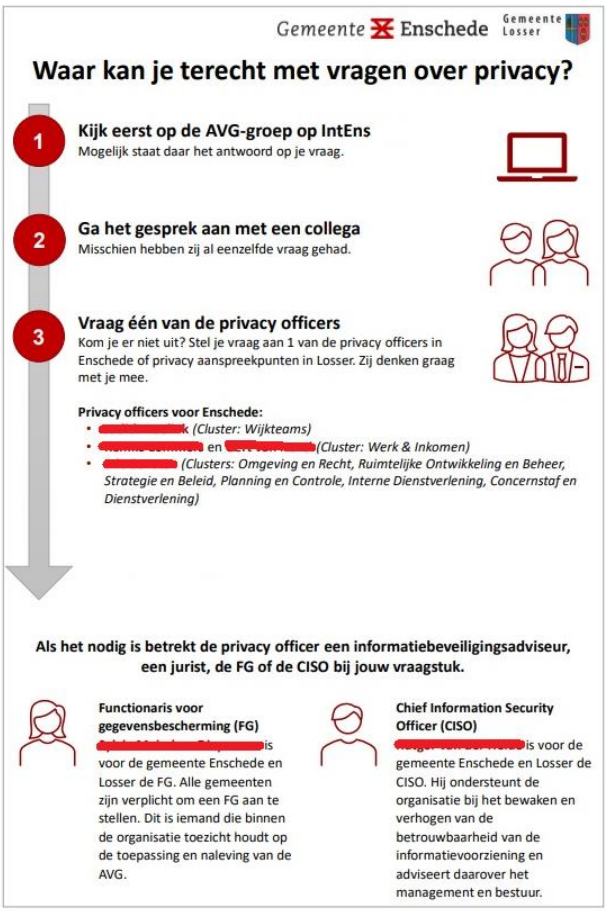
Voor een goede en juiste uitvoering is het van belang dat iedereen binnen de organisatie op de hoogte is van de beginselen van de AVG en het belang van aandacht voor de bescherming van persoonsgegevens.
Organisatorische inbedding betekent het toewijzen van taken, verantwoordelijkheden en bevoegdheden en bewustzijn creëren.

Er is in 2023 veel aandacht geweest voor het uitbalanceren en positioneren van het privacy team.
Wekelijks vindt een onderling overleg plaats over de rollen/taken van het team dat primair betrokken is bij privacy zaken. De privacy officers, CISO en FG nemen deel aan dit overleg.

In breder verband kent de gemeente (Enschede) de Adviescommissie informatiebeveiliging en privacybescherming. Deze multidisciplinaire commissie komt tweemaandelijks bij elkaar behandelt o.a. privacy in breder verband.

[5] De gegevensbeschermingseffectbeoordeling wordt ook wel afgekort tot DPIA naar de Engelse term Data Protection Impact Assessment.

Ter informatie van de organisatie zijn er regelmatig berichten op intranet geplaatst zoals infographics waarin wordt uitgelegd hoe de rollen zijn verdeeld.



RECHTEN VAN BETROKKENEN

De gemeente dient degene van wie zij de persoonsgegevens verwerkt (betrokkene) zowel actief als passief te informeren over het verwerken, de wijze van het verwerken, de grondslag en de maatregelen die zij neemt om onrechtmatige toegang en -verwerking te voorkomen. Daarnaast stelt de AVG betrokkenen in staat om middels een aantal rechten controle en invloed uit te oefenen over zijn of haar persoonsgegevens. We noemen dit een AVG-verzoek.

De ingekomen AVG-verzoeken rondom de uitoefening van rechten worden doorgezet naar de betrokken vakafdeling en worden waar nodig besproken in het wekelijkse privacy overleg (zie verder onder 2). De privacy officers kunnen de vakafdelingen bij het proces van het beoordelen en behandelen van de AVG-verzoeken begeleiden. Zie verder hoofdstuk 5 ‘rechten van betrokkenen’

SAMENWERKING

De gemeente werkt op meerdere beleidsterreinen, in verschillende bedrijfsfuncties, in diverse rollen en hoedanigheden samen met (mede) overheden en private organisaties. In veelvoorkomende gevallen zal er sprake zijn van een verwerking van persoonsgegevens tussen partijen: ontvangen van persoonsgegevens, verzenden van persoonsgegevens, maar ook het opslaan van en inzage hebben in persoonsgegevens valt onder dit begrip. Deze verwerkingen dienen ook te voldoen aan de AVG. Het is de verantwoordelijkheid van de gemeente Enschede om hierover met deze andere partijen afspraken te maken. In geval van het delen van persoonsgegevens en andere (gevoelige) informatie is dit ook in vrijwel alle gevallen gebeurd.

Een belangrijk aandachtspunt is hierbij wel dat deze afspraken periodiek dienen te worden herzien op actualiteit Samenwerkingen veranderen in de loop van de tijd, gegevensuitwisselingen veranderen, soms op basis van behoefte, soms op basis van veranderende wet- en regelgeving. Dat kan invloed hebben op de gemaakte afspraken. Een voorbeeld van een belangrijke samenwerkingspartij waarmee gevoelige gegevens worden gedeeld is het Kennispunt Twente. Hierbij zijn een drietal DPIA’s in uitvoering en de FG heeft in samenwerking met de FG’s van Almelo en Hengelo aanbevelingen gegeven over hoe samenwerkingsafspraken ten aanzien van AVG-governance en AVG-compliancy beter vormgegeven kunnen worden. Een ander voorbeeld is IT-knooppunt

Twente. De gemeente Enschede levert hierbij diensten aan vrijwel alle Twentse gemeenten. Hierbij is een DPIA in uitvoering en bijna voltooid en er is een nieuwe verwerkersovereenkomst opgesteld.

Op het gebied van samenwerking is nog werk te verzetten. Dit is ook als aandachtspunt voor 2024 benoemd. Dit is nodig omdat de verwachtingen van burgers toenemen en de verwachtingen en verantwoordelijkheden van de gemeente na ruim vijf jaar AVG zich steeds verder en beter uitkristalliseren waarbij het mogelijk wordt en noodzakelijk is om een verdere professionaliseringslag te maken. Met name de wetgeving binnen het sociaal domein is hierbij lastig te interpreteren. De WMO en Jeugdwet, die in 2015 in werking traden (vóór het bestaan van de AVG) zijn hierin lastig omdat deze wetten niet specifiek genoeg zijn ten aanzien van hetgeen gedeeld mag worden. Dit maakt maatwerk in iedere nieuwe situatie nodige en dit vraag het nodige van de medewerkers. De privacy officers bieden hierbij veel begeleiding en hebben samen met de vakafdelingen afspraken gemaakt over zorgvuldig werken binnen de AVG. Daarnaast hebben de vakafdelingen aangegeven behoefte te hebben aan meer kaders ten aanzien van wat nodig is om een samenwerking goed en veilig vorm te geven. Privacy officers en FG werken hierbij samen om in deze informatiebehoefte te voorzien

BEVEILIGING

Het is essentieel dat de gemeente passende technische en organisatorische maatregelen neemt ter beveiliging van persoonsgegevens. Wat passend is hangt af van onder andere de specifieke verwerkingen en de risico's die deze met zich meebrengen en de kwetsbare onderdelen in het proces van de verwerkingen. Bij het bepalen van wat passend is wordt rekening gehouden met de gevoeligheid van de gegevens, dat de te treffen maatregelen in verhouding staan tot de risico's (op basis van een risicoanalyse), van wat technisch mogelijk is en de kosten hiervan. Vervolgens moet gezocht worden naar een balans tussen het risiconiveau en de maatregelen.
Ten aanzien van technische en organisatorische maatregelen wordt verwezen naar de ENSIA-rapportage die jaarlijks met het College en de Raad worden gedeeld.
Daarnaast geldt er onder de AVG een meldplicht datalekken. Dit houdt in dat incidenten, waaronder inbreuken op de beveiliging, onderzocht worden en onder omstandigheden gemeld worden aan de AP en/of de betrokkene(n).

In het voorjaar van 2023 heeft de gemeente Enschede twee groepen van de Haagse Hogeschool gevraagd om een zogenaamde 'social engineering aanval' te organiseren. Dit hebben zij gedaan in de vorm van een 'Mystery Guest' bezoek aan het stadhuis en aan het stadskantoor. De zwakte schakel in de beveiliging is immers vaak de mens. De studenten hebben daarbij een aantal kwetsbaarheden gesignaleerd die zij hebben beschreven in een rapportage met daarbij aanbevelingen om hierin verbeteringen aan te brengen. Globaal was hun bevinding dat de Enschedese Ambtenaar te 'lief en gastvrij' is. De aanbevelingen om de Security Awareness te vergroten zijn gedeeld met het management en acties zijn ingezet.

Een punt van aandacht is werken vanuit het buitenland. Meerdere keren per jaar vragen medewerkers om toestemming om vanaf een ander land te mogen werken. Zolang dit binnen de Europese Economische Ruimte (EER) plaatsvind is dit geen probleem aangezien de bescherming van persoonsgegevens dan op dezelfde wijze geregeld is volgend de AVG. Voor een aantal andere landen heeft de Europese Commissie (EC) een adequaatheidsbesluit genomen (artikel 45 van de AVG). De EC stelt dan vast dat de gegevensbescherming in dat land van een vergelijkbaar niveau is als de AVG. Wanneer een land op deze lijst voorkomt is het werken vanuit dat

land ook als veilig aan te merken. Is dat niet het geval dan zijn mogelijk aanvullende maatregelen nodig, of volgt een negatief advies. Op advies van de FG en CISO worden de mogelijkheden en onmogelijkheden t.a.v. het werken in het buitenland op dit moment in samenwerking met P&O en Juridische zaken verder uitgewerkt in beleid.

Een ander punt van zorg is het gebruik van Zorgmail. Dit is een veilige mailtoepassing om gevoelige informatie of bijzonder persoonsgegevens veilig via de mail te kunnen versturen. Binnen deze toepassing is op dit moment geen twee factor authenticatie ingericht. Dit is nodig om er zeker van te kunnen zijn dat de mail ook inderdaad door de juiste persoon wordt ontvangen. Daarnaast is bij deze mailtoepassing de herkenbaarheid van de mail, als afkomstig van de gemeente een aandachtspunt. Het moet ook voor de ontvanger helder zijn dat deze mail inderdaad van de gemeente afkomstig is op basis van onder andere de herkenbaarheid c.q. huisstijl. De FG en CISO hebben hierin aanbevelingen voor verbeteringen in gedaan.

VERANTWOORDING

De AVG legt de verantwoordelijkheid bij de organisatie zelf om aantoonbaar te maken dat deze voldoet aan de privacyregels. De organisatie heeft hierbij een verantwoordingsplicht. Door aan deze plicht te voldoen, levert de organisatie een belangrijke bijdrage aan de bescherming van het grondrecht van mensen op privacy. Dit betekent dat het college van B&W aan moet kunnen tonen dat de verwerkingen van persoonsgegevens voldoen aan de beginselen van de AVG en aan de relevante wet- en regelgeving.

De werkzaamheden die worden verricht op het vlak van privacy (en informatiebeveiliging) worden gedocumenteerd. Denk aan de wekelijkse werkoverleggen, de adviescommissie informatieveiligheid en privacy en gesprekken met het management. Daarnaast heeft de FG periodieke overleggen met de Gemeentesecretaris en de portefeuille houdend wethouder. Deze overleggen zijn ingepland per kwartaal en worden tevens spontaan belegd waar nodig. Als laatste voert de FG periodiek gesprekken met business controllers en de strategisch adviseur ten aanzien van risicomanagement, onder andere ten behoeve van de jaarrekening 2023

Er zijn ook nieuwe of geactualiseerde initiatieven. Denk aan het gebruik van het Borgingsproduct 3.0 van de VNG. Dit is een toetsingskader waarmee de organisatie kan toetsen in hoeverre zij in staat is om de naleving van de AVG te waarborgen. Deze wordt ingezet als jaarlijkse meting. Daarnaast maken de privacyofficers een jaarplan en ook dit jaarverslag en het toezichtsplan van de FG zijn input voor de organisatie om te toetsen in hoeverre zij als organisatie aan de AVG voldoet en waar nog actiepunten liggen om in het komende jaar op te pakken. Evenals dit jaar zullen deze documenten ook komend jaar in de jaarlijkse cyclus worden gebruikt.

CONCLUSIE

In 2023 heeft de gemeente verschillende verbeterslagen gemaakt waarbij de gegevensbescherming verder is geprofessionaliseerd. Positieve ontwikkelingen waren bijvoorbeeld het onder de loep nemen van een aantal processen, waaronder het DPIA-proces, maar ook het maken van nieuw beleid op een aantal onderwerpen en nieuwe formats om meer uniform te kunnen werken en fouten te voorkomen.
Er zijn ook aandachtspunten voor de organisatie om aantoonbaar te kunnen voldoen aan de AVG. In het tweede deel van de rapportage worden aanbevelingen gedaan om gegevensbescherming verder te verankeren in de organisatie.

Hieronder wordt dit verder gevisualiseerd. (Het kopje beveiliging heeft betrekking op datalekken. Voor beveiliging wordt verwezen naar de ENSIA-rapportage). Er is ook een verwachting opgenomen voor 2023. Die wordt in het volgende hoofdstuk onderbouwd.

2. VERWERKINGSREGISTER

De verantwoordingsplicht binnen de AVG houdt onder andere in dat een organisatie moet kunnen aantonen dat een verwerking van persoonsgegevens voldoet aan de belangrijkste uitgangspunten van de AVG. Ook moet een organisatie kunnen laten zien welke gegevens worden verwerkt en dat de juiste technische en organisatorische maatregelen zijn genomen om de persoonsgegevens te beveiligen. In de AVG staat een aantal verplichte maatregelen genoemd waarmee een organisatie kan laten zien dat zij aan haar verantwoordingsplicht voldoet. Een daarvan is het bijhouden van een verwerkingenregister.

Eind 2021 is een project gestart om het verwerkingsregister (van de gemeente Enschede) te actualiseren. De opstart van dit project verliep aanvankelijk moeizaam. Na de zomer van 2022 zijn echter grote stappen gemaakt. Eind 2022 zijn alle belangrijke verwerkingen geïnventariseerd. De resterende processen werden begin 2023 geïnventariseerd. Daarna is, zoals was afgesproken, in het projectplan een procedure vastgesteld om het register actueel te kunnen blijven houden. De nieuw aan te stellen AVG-coördinator zal daar een coördinerende en begeleidende rol in gaan spelen. Een publieksvriendelijke versie van het verwerkingenregister is gepubliceerd op de website van de gemeente.

De interim FG is in 2022 betrokken geweest bij de selectie van categorieën informatie die in het register opgenomen dienen te worden. De huidige FG constateert dat samenwerkingsverbanden waar de gemeente aan deelneemt nog niet zijn opgenomen in dit register. De FG beveelt aan om deze verwerkingen in 2024 aan te vullen in het verwerkingenregister. Daarnaast mist het register 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. Het advies van de FG is om deze in 2024 uit te voeren. Daarnaast is het nodig om het digitale systeem aan te passen zodat deze informatie toegevoegd kan worden in het verwerkingenregister en om hieruit de nodige managementinformatie te kunnen genereren.

3. DPIA’S

DPIA’s, ofwel Data Protection Impact Assessments, spelen een cruciale rol bij het borgen van privacybescherming. De beste bescherming wordt in de praktijk geboden wanneer technische en organisatorische maatregelen worden getroffen om te voorkomen dat bepaalde risico’s zich voordoen. Door middel van een DPIA worden systematisch alle risico’s en de impact daarvan, voor zowel de gemeente als organisatie als voor de inwoners waarvan we de gegevens verwerken, in kaart gebracht. Vervolgens wordt voor elk van de risico’s de impact beoordeeld en welke mitigerende maatregelen kunnen worden toegepast. Een DPIA is in principe ook het systematisch nalopen of de AVG-beginselen, waaronder data-minimalisatie, proportionaliteit en subsidiariteit en privacy by design, zijn toegepast.

Als organisatie wil en moet gemeente Enschede inzicht hebben in de (privacy-)risico's van onze data-verwerkende processen. Dit is nodig om de (privacy-) belangen van betrokkenen (bijvoorbeeld inwoners, maar ook eigen medewerkers) te kunnen beschermen. Maar ook om de belangen van de gemeente te waarborgen: denk aan reputatieschade of aantasting van relaties met partners, door een privacy-inbreuk. Dit inzicht kan alleen verkregen worden door een gerichte inventarisatie en risicoanalyse van die processen. Dat is het doel van een DPIA.

Daar komt bij dat bij processen met hoge privacy-risico's voor betrokkenen het uitvoeren van een DPIA geen keuze is maar een wettelijke verplichting. Niet nakomen van deze verplichting kan leiden tot hoge boetes van de Autoriteit Persoonsgegevens (AP).

Binnen de gemeenten Enschede zijn de afgelopen periode stappen gezet om de DPIA meer voor het voetlicht te brengen en, waar nodig en verplicht, een DPIA uit te voeren. Dit komt langzaam op gang, maar de bewustwording groeit. Maar om dit proces nog een extra boost te kunnen geven is meer nodig. De FG heeft daarom het advies gegeven om:

1. Te investeren in de kennis van ambtenaren die DPIA's uitvoeren of hierbij inhoudelijk betrokken zijn;
2. Te investeren in de kennis van privacy officers in hun rol van procesbegeleiders bij het uitvoeren van een DPIA;
3. De procedure en het beleid voor het uitvoeren van DPIA's te actualiseren;
4. Om standaard formats te gebruiken voor het uitvoeren van DPIA's en deze te voorzien van praktische handleidingen;
5. Het DPIA-proces digitaal te ondersteunen en de rapportages zakelijk te archiveren;
6. De informatie uit een DPIA te gebruiken bij het opstellen van een verwerkersovereenkomst;
7. De informatie uit een DPIA te gebruiken bij het actueel houden van het verwerkingenregister.

Gemeente Enschede heeft hier goede actie in uitgezet die hebben geleid tot de volgende acties:

1. Voor de bijscholing van privacy officers en overige ambtenaren die betrokken zijn bij de uitvoering van DPIA's is op advies van de FG een incompany training ingekocht. Inmiddels zijn 32 medewerkers geschoold. In 2024 worden meer scholingen georganiseerd;
2. Alle privacy officers hebben de DPIA-scholing gevolgd en begeleiden op dit moment meerdere DPIA-processen en teams die DPIA's uitvoeren;
3. De procedure en het beleid zijn geactualiseerd en beschikbaar via IntEns (intranet);
4. De formats en de toelichtingsdocumenten zijn ontwikkeld en beschikbaar via IntEns (intranet). Op moment van schrijven worden acties uitgezet om deze beschikbaar te maken via SmartDocuments;
5. Zakelijke archiveren is binnenkort mogelijk. Hier wordt op moment van schrijven de laatste hand aan gelegd;
6. Het kunnen gebruiken van de informatie uit de DPIA voor de verwerkersovereenkomst is opgenomen in zowel de DPIA procedures als in de nieuwe aanbestedingsprocedure;
7. Het gebruiken van de informatie uit de DPIA voor het actueel houden van het verwerkingenregister is opgenomen in zowel de DPIA procedure als in de procedure actueel houden verwerkingenregister.

Het afgelopen jaar zijn beduidend meer DPIA's gestart/uitgevoerd dan in de jaren hiervoor. De medewerkers van de gemeente blijken inmiddels beter bewust en bekend met de noodzaak tot het uitvoeren van een DPIA, maar toch is dat nog niet voor alle organisatieonderdelen het geval. Er zal ook in 2024 veel gecommuniceerd moeten worden over de noodzaak tot het uitvoeren van een DPIA en over de wijze waarop hierbij hulp kan worden

gekregen in de vorm van scholing en door begeleiding van het proces door de privacy officer. Daarnaast is het nodig om de effectiviteit van de mitigerende maatregelen aangaande risico's die zijn benoemd in de DPIA te beoordelen en te borgen dat DPIA's periodiek worden gereviewd. Hiervoor zijn nog aanvullende acties nodig.

Voor een overzicht van alle uitgevoerde DPIA's worden verwezen naar **Bijlage 1**.

4. UITOEFENING RECHTEN DOOR BETROKKENEN

Op dit moment loopt het afhandelen van met name uitgebreide, complexe en/of domein overstijgende AVG-verzoeken nog niet in alle gevallen gladjes. Het gaat om een beperkt, maar toch toenemend aantal verzoeken per jaar (in 2022 minder dan 10; in 2023 meer dan 20 van de in totaal 44 verzoeken). Deze domein overstijgende verzoeken betreffen vooral het sociaal domein, zijn meestal erg arbeidsintensief en worden - op dit moment nog - ad hoc opgepakt en gecoördineerd.

In 2022 is heeft de FG aangegeven dat dat uit gesprekken bleek dat alle verzoeken tijdig waren gehonoreerd, af en toe onder gebruikmaking van de mogelijkheid tot verlenging. Er zijn geen klachten binnengekomen over ondeugdelijke of niet tijdige afhandeling. In 2023 zijn echter meerdere ingebrekestellingen ontvangen in verband met niet tijdige afhandeling.

De FG heeft aanbevelingen gedaan over hoe dit proces rond het faciliteren van betrokkenen in het uitoefenen van hun rechten beter gestroomlijnd en geborgd kan worden. De gemeentelijke organisatie heeft op basis daarvan een aantal acties ondernomen:

- Het college vragen om binnen de zomernota financiële ruimte te creëren voor het aanstellen van een AVG-coördinator in 2024. Het college en de raad zijn hiermee akkoord gegaan waardoor de AVG-coördinator geworven kan gaan worden;
- Het mogelijk maken voor betrokkenen om online via een webformulier een AVG-verzoek te kunnen doen waarbij ook meteen de scope van het verzoek kan worden toegelicht en via DigiD authenticatie eenvoudig en veilig de identiteit van de betrokkene kan worden gecontroleerd;
- Zaakgerichte archivering in het gemeente brede document management systeem van de verzoeken en bewaking van reactietermijnen;
- Betere juridische toetsing van het verzoek waar nodig;
- Heldere formats (voor het versturen van):
    - de ontvangstbevestiging;
    - aankondiging van de schorsing van het verzoek;
    - aangeven dat gebruik gemaakt wordt van de mogelijkheid tot verlenging van de reactietermijn;
    - het formuleren van een besluit.

Op moment van het schrijven van dit jaarverslag zijn bovenstaande acties in uitvoering en zullen in 2024 in werking worden genomen. Een en ander is voor een groot deel wel afhankelijke van de aanstelling van de AVG-coördinator. De FG wil hierbij dringen adviseren dit op korte termijn te realiseren.

In **Bijlage 2** is een overzicht opgenomen van het aantal verzoeken van betrokkenen voor het jaar 2023. Daaronder vallen ook de klachten van betrokkenen.

5. DATALEKKEN

Datalekken worden binnen de gemeente Enschede afgehandeld volgens het protocol datalekken dat in 2021 is vastgesteld. In dit protocol is voorzien in een coördinerende rol voor één van de dienstdoende securityadviseurs. In geval van hoge urgentie of twijfel, dient volgens dit protocol de FG te worden betrokken. Dat wordt met regelmaat en tijdig gedaan.
Opvallende datalekken waarbij de FG een actieve rol heeft gehad betreffen een datalek rondom de verkoop van archiefkasten waarbij nog een aantal oude documenten zijn aangetroffen door de koper. Alle stukken zijn door de koper aan de gemeente teruggegeven. Daarnaast zijn er enkele datalekken geweest die het noodzakelijk maakten om afspraken strakker in te regelen of aanvullende informatie te geven aan medewerkers over hoe met een bepaalde situatie om te gaan. Een voorbeeld daarvan is bijvoorbeeld wanneer een BOA handhaving openbare ruimte iemand wel of niet een ID-bewijs mag vragen te tonen en wat de voorwaarden zijn ten aanzien van het doorgeven van deze persoonsgegevens.

Over het geheel gezien worden de meeste datalekken veroorzaakt door menselijke fouten. In de meeste gevallen gaat het dan om persoonsgegevens die zijn verstuurd aan de verkeerde ontvanger, vaak doordat een verkeerde bijlage is bijgevoegd. Om nog meer te kunnen leren uit datalekken is het van belang dat datalekken worden afgehandeld door privacy officers. Zij kunnen de afdelingen helpen om na te gaan waardoor een fout is gemaakt en samen met de betrokkenen nagaan welke mogelijkheden er zijn om een en ander zo in te richten dat de kans op het optreden van een datalek zo klein mogelijk wordt. Om dat te kunnen realiseren is een herziening van de procedure nodig en is een uitbreiding van de capaciteit bij de privacy officers noodzakelijk. Beide kunnen worden gerealiseerd. De nieuwe procedure is vastgesteld waarbij is opgenomen dat datalekken worden afgehandeld door de privacy officers. Daarnaast is een capaciteitsuitbreiding van de privacy officers goedgekeurd door het college in de zomernota. De nieuwe procedure gaat naar verwachting in per 1 maart en de verwachting is ook dat de capaciteitsuitbreiding bij de privacy officers dan is gerealiseerd.
Om goed te kunnen sturen op de datalekken en beveiligingsincidenten moet de registratie verbetert worden. In de Datalekken- en beveiligingsincidenten rapportage over 2023 stellen de FG en CISO aantal verbeterpunten voor.

In **Bijlage 3** is een beknopt overzicht opgenomen van het aantal en de soort datalekken in 2023. Voor het totale overzicht met toelichting hierop wordt verwezen naar de Datalekken- en beveiligingsincidenten rapportage over 2023

6. BEWUSTWORDING

Om te zorgen voor bewustwording worden verschillende activiteiten ontplooid.
Er worden regelmatig berichten geplaatst op intranet, zoals bijvoorbeeld veilig werken tijdens de zomervakantie.
De gemeente maakt gebruik van een e-learning om te zorgen informatieveilig gedrag. Het e-learning pakket bestaat uit verschillende onderwerpen zoals phishing, social engineering, datalekken en aandacht voor de werkplek. Het pakket wordt geleverd door een genormeerde partij. De deelname aan het programma laat voor dit jaar echter te wensen over (circa 30%). Daarnaast is behoefte aan meer op de medewerker afgestemde informatie. Daarom is een nieuw aanbestedingstraject gestart om een meer passende vorm van e-learning te kunnen gaan bieden. Dit traject verloopt niet snel, omdat IT te maken heeft met een vol projectenportfolio en hoge werkdruk.

Deze omstandigheden hebben geleid tot de vertraging waar de FG en de Chief Information Security Officer (CISO) zich zorgen over maken. Bewustmaking en opleiding van medewerkers is voor een organisatie immers niet vrijblijvend (art. 39 b AVG).
Daarnaast zijn de regels voor veilig werken geactualiseerd. Hierin is aandacht van privacy een onderdeel. Dit wordt begin 2024 met de organisatie gedeeld. Gelijktijdig is divers bewustwordingsmateriaal opgefrist en in de nieuwe huisstijl van de gemeente gezet. Dit wordt eveneens in 2024 gebruikt voor de bewustwordingscampagne.
Bepaalde groepen medewerkers hebben behoefte aan meer verdieping op onderwerpen zoals:

- Wanneer een verwerkersovereenkomst moet worden afgesloten en wat daarbij van belang is;
- Welke informatie nodig is voor het opstellen van het verwerkingenregister;
- Waar op gelet moet worden bij het aangaan van samenwerkingsverbanden vanuit AVG perspectief;
- Wanneer informatie wel of niet mag worden gedeeld en welk afwegingskader daarbij kan worden gebruikt;
- Hoe een DPIA uit te voeren en wanneer dit verplicht is.

Voor een deel kan hierbij informatie gegeven worden via e-learning, voor andere onderwerpen zijn andere onderwijsvormen beter geschikt, zoals incompany trainingen of cursussen. Een mooi voorbeeld daarvan zijn de DPIA-trainingen die in 2023 zijn georganiseerd en welke een vervolg krijgen in 2024.
Naast e-learningen en scholingen wordt bij verschillende gelegenheden uitleg en instructie gegeven. Voorbeelden hiervan zijn het aanschuiven tijdens teamoverleggen of de presentatie datagedreven werken en privacy.
Daarnaast is een werkgroep bezig met het opstellen van een jaarkalender waarbij gedurende het jaar verschillende bewustwordingsactiviteiten kunnen worden aangeboden.

7. TRANSPARANTIE

De gemeente probeert transparant te zijn rondom de verwerking van persoonsgegevens.
Medio 2022 is een nieuwe privacyverklaring opgesteld. Begin 2023 is de geactualiseerde versie van het verwerkingsregister geplaatst. Daarnaast wordt er op dit moment gewerkt aan het updaten van de informatie over privacy en gegevensbescherming op de website van de gemeente Enschede. Er zijn nieuwe en uitgebreidere teksten geschreven over verschillende privacy-gerelateerde onderwerpen zoals het verwerken van persoonsgegevens door de gemeente, het verwerkingenregister, datalekken, privacyrechten, het gebruik van camera's in de stad en wetgeving. Tevens wordt het mogelijk gemaakt om digitaal een AVG-verzoek in te dienen en realiseren we de mogelijkheid om een datalek 24/7 digitaal te kunnen melden.
Met name met het publiceren van het verwerkingenregister geeft de gemeente veel informatie over welke gegevens in welke situatie worden verzameld, met welk doel en wat daarvan de bewaartermijn is. Ook wordt er actief verwezen naar de toepasselijke landelijke voorzieningen zoals de website: ''Wie gebruikt mijn gegevens bij de overheid?"

8. WET POLITIEGEGEVENS (WPG)

Gemeenten (en andere werkgevers) die buitengewoon opsporingsambtenaren (boa's) in dienst hebben en gegevens verwerken op grond van de Wet Politiegegevens, zijn op grond van deze wet verplicht om jaarlijks een interne audit uit te voeren. Eens in de vier jaar moet daarnaast een externe audit worden uitgevoegd. Dit is een nieuwe verplichting. In 2022 is deze externe audit uitgevoerd en de rapportage daarvan is ingediend bij de Autoriteit Persoonsgegevens.

Het onderzoek is uitgevoerd naar strafrechtelijke handhaving in het kader van 1) en openbare ruimte en 2) de Leerplichtwet. De externe auditor heeft "*vastgesteld dat gemeente Enschede niet (geheel) voldoet aan het bij of krachtens de wet bepaalde. Inzake de uitvoering van de hercontroles, bevelen wij gemeente Enschede aan om deze door een externe auditor te laten uitvoeren*".

Uit het rapport bleek dat er verschillende aandachtpunten zijn, waaronder:

- Bijzondere categorieën van politiegegevens;
- Verwerker en Verwerkersovereenkomst;
- Bewaartermijnen, verwijderen en vernietigen;
- Verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee;
- Documentatie;
- Audits en logging;
- Gegevensbescherming door standaardinstellingen/DPIA's.

Op basis van de aanbevelingen van de auditor heeft de gemeente Enschede een verbeterplan opgesteld. De FG is hierbij betrokken geweest en is periodiek om advies gevraagd. Daarnaast heeft de FG periodiek evaluatiegesprekken gepland om toezicht te kunnen houden op de voortgang van het verbeterplan.

De resultaten van deze verbeteringen worden opnieuw door de externe auditor beoordeeld. De rapportage wordt begin 2024 verwacht en deze rapportage moet uiterlijk 1 maart worden aangeleverd aan de Autoriteit Persoonsgegevens.

Toezicht door de Functionaris Gegevensbescherming op naleving van de Wpg

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.

STAND VAN ZAKEN DECEMBER 2023

1. Wpg beleid: Op basis van de VNG modellen is Wpg beleid voor de gemeente Enschede opgesteld en vastgesteld;
2. De bewustwordingsverplichting: de leidinggevenden en operationeel experts van beide domeinen 1) openbare ruimte en 2) de leerplichtwet zijn hier met hun teams mee bezig. Bij leerplicht is er een instructie gegevens door een extern bureau en hebben ze een werkinstructie op papier. Om dit jaarlijks te doen zijn verkennende stappen gezet richting periodieke e-learning;
3. Het autorisatieproces met betrekking tot het vastleggen van politiegegevens: er is een softwarepakket beschikbaar waarin dit verder is vormgegeven;
4. De kwaliteit en waarborging van de juistheid van de nauwkeurigheid van politiegegevens: na de volledige inrichting van de betreffende softwareomgevingen kan dit worden gecontroleerd;
5. Het verwerken van politiegegevens: in de softwarepakketten kan op basis van labelling van de gegevens (art. 8 gegevens of art. 9 gegevens) worden nagegaan in hoeverre deze rechtmatig zijn verwerkt. Dit is ingericht;
6. De bewaartermijnen: de wettelijke bewaartermijnen die gelden voor politiegegevens zijn bekend en worden middels de softwaretoepassing bewaakt;
7. Het ter beschikking stellen en verstrekken van politiegegevens: ook dit is digitaal ingericht en hierbij kan nagegaan worden met welke ontvangers de gegevens rechtmatig worden gedeeld;
8. De controle op de informatiebeveiliging en de controle op het uitvoeren van een risicoanalyse: dit is geregeld via de informatieveiligheidsspecialisten en e.e.a. wordt meegenomen in de te organiseren audits. Een DPIA is daarbij ook een vorm van risicoanalyse. In het toezichtsplan van de FG heeft het onderwerp DPIA (uitvoeren waar dit wettelijk verplicht is) extra aandacht gekregen. Een aantal acties t.a.v. het actualiseren van het DPIA beleid, het investeren in kennis over het uitvoeren van DPIA's in de diverse domeinen en het werken op een uniforme wijze waarbij een pragmatische aanpak kan worden gevolgd, zijn inmiddels in gang gezet;
9. Het register voor verwerkingen: deze is in 2023 geactualiseerd en hierin zijn ook alle verwerkingen die vallen onder de Wpg meegenomen;
10. De verplichtingen ten aanzien van de hercontrole en de interne audit: de rapportage wordt begin januari 2014 verwacht en moet uiterlijk 1 maart 2024 zijn aangeleverd aan de Autoriteit Persoonsgegevens. Daarnaast heeft de gemeente besloten om twee interne medewerkers op te leiden tot interne auditor;
11. Periodieke rapportages: afgesproken dat is de FG deze rapportage opneemt in het jaarverslag. Daarnaast heeft de FG minimaal ieder kwartaal een gesprek met de gemeentesecretaris en met de portefeuille houdend wethouder, waarin deze worden bijgepraat over de voortgang en ontwikkelingen. Waar nodig word dit met inhoudelijke notities aangevuld. Voor tussentijdse urgente zaken geldt het open deur principe.

9. OVERIG

De Algemene Verordening Gegevensbescherming (AVG) geeft regels en verplichtingen ten aanzien van het verwerken van persoonsgegevens. De wet verbindt duidelijke eisen aan de positionering van een FG. Zo is het essentieel dat de FG onafhankelijk kan toezien op de naleving van de AVG in de betreffende organisatie. Naast de wettelijke bepalingen heeft de Autoriteit Persoonsgegevens (AP) ook concrete uitgangspunten opgesteld over

onder meer de informatiepositie van de FG, de middelen die de FG nodig heeft en de toegang van de FG tot het bestuur van de organisatie.

Deze uitgangspunten zijn verwerkt in een ‘Reglement voor de Functionaris Gegevensbescherming” welke op 29 maart is vastgesteld in het college van burgemeester en wethouders en op 15 mei in de Gemeenteraad is vastgesteld. In dit reglement is de landelijke regelgeving vertaald naar de gemeentelijke organisatie geeft de kaders weer voor de wijze waarop de FG van de gemeente de taken en bevoegdheden onafhankelijk en zonder enige belemmering kan uitoefenen. Het reglement is 26 mei gepubliceerd in het gemeenteblad van Enschede en op de website lokaleregelgeving.overheid.nl.

De FG heeft dit jaar deelgenomen aan het wekelijkse overleg met de privacy officers, de adviescommissie informatieveiligheid en privacy, de overleggen met juridische zaken en het regionale FG-overleg. Daarnaast heeft regelmatig informeel overleg plaatsgevonden met de privacy officers, CISO en CIO. Verder heeft afstemming plaatsgevonden met externe partijen zoals FG’s/PO’s van andere gemeenten of van samenwerkingspartners.

De FG heeft daarnaast deelgenomen aan diverse (digitale) bijeenkomsten van VNG/IBD zoals bijeenkomsten rondom de Wams, aandachtspunten in het sociaal domein en kennissessies over de Wpg.

Ten aanzien van Kennisbevordering heeft de FG deelgenomen aan diverse (bij-)scholingsactiviteiten en cursussen.

DEEL 2: VOORUITKIJKEN NAAR 2024

Op basis van de bevindingen over 2023 doet de FG de volgende aanbevelingen. De aanbevelingen zijn ‘risico gebaseerd’. Er wordt tevens rekening gehouden met de impact op de organisatie om aan de gestelde aanbeveling te voldoen.

TOP 5 AANBEVELINGEN

Om de aanbevelingen overzichtelijk te houden wordt gewerkt met een top 5 van belangrijkste aanbevelingen.

AANBEVELING1

Samenwerkingsverbanden in kaart brengen en controleren.

De Autoriteit Persoonsgegevens heeft samenwerkingsverbanden binnen de (digitale) overheid benoemd als één van haar aandachtsgebieden voor 2024. De Autoriteit Persoonsgegevens geeft in haar eigen jaarplan aan dat zij opnieuw aandacht besteden aan het delen van gegevens tussen verschillende onderdelen van de overheid en andere organisaties. Dit is gezien de gevoelige informatie die gemeenten met samenwerkingspartners delen en ontwikkelingen op landelijk en internationaal gebied, terecht een punt van aandacht.
De Functionaris Gegevensbescherming dringt er daarom op aan om in 2024:

- na te gaan of het overzicht van samenwerkingsverbanden nog actueel is;
- daarbij te kijken naar de onderliggende zaken die van belang zijn in het kader van AVG compliance:
    - is helder wat het doel is van het samenwerkingsverband, wie er aan deelnemen en wat de afspraken zijn ten aanzien van aanlevering en verstrekking van data/persoonsgegevens?
    - wordt hierbij voldaan aan de wettelijke criteria?
    - hoe zijn de verantwoordelijkheden verdeeld binnen het samenwerkingsverband zoals (mede)verantwoordelijke of verwerker)?
    - hoe zijn binnen het samenwerkingsverband de rechten van betrokkenen geborgd?
    - hoe wordt vormgegeven aan beginselen als proportionaliteit en subsidiariteit, toetsbaarheid en transparantie en dataminimalisatie?
    - welke beveiligingsmaatregelen zijn getroffen en hoe is de toegang tot de informatie ingericht (autorisaties).
- op basis van de uitkomst van bovenstaande alle benodigde acties in gang te zetten die nodig zijn om waar nodig verbeteringen aan te brengen.

AANBEVELING2

Rechten van betrokkenen beter faciliteren.

Zoals eerder aangegeven heeft de FG in 2023 aanbevelingen gedaan over hoe het proces rond het faciliteren van betrokkenen in het uitoefenen van hun rechten beter gestroomlijnd en geborgd kan worden. Het college heeft binnen de zomernota financiële ruimte gecreëerd voor het aanstellen van een AVG-coördinator. De AVG coördinator dient een belangrijke rol te vervullen bij het coördineren en afhandelen van AVG-verzoeken, zoals het in ontvangst nemen van het verzoek, de identiteitscontrole, het helder krijgen van de scope van het verzoek, het (tijdig) versturen van een ontvangstbevestiging, besluit, waar nodig aangeven dat uitstel van toepassing is, afstemmen met Juridische zaken en het bewaken van de reactietermijnen.

Het is van belang deze functionaris niet alleen op korte termijn te werven maar ook juist en centraal te positioneren en te voorzien van alle bevoegdheden die nodig zijn voor de invulling van deze taak. Frequent overleg met de privacy officers is hier tevens bij van belang.
Ter voorbereiding hierop wordt de procedure hiervoor herzien waarnaar de AVG-coördinator hier invulling aan kan geven.
De Functionaris Gegevensbescherming wijst er op dat het van belang is dat op korte termijn een AVG-coördinator wordt geworven zodat de noodzakelijke verbeteringen aangebracht kunnen worden en in werking kunnen worden gesteld.

AANBEVELING 3

Actueel houden van het verwerkingenregister

Medio 2023 is een procedure 'Actueel houden van het verwerkingenregister' vastgesteld. Het is van belang hierover te blijven communiceren. Alle processen en datastromen binnen de gemeente zijn immers continu aan veranderingen onderhevig. De ene keer komt dit door interne wijzigingen, de andere keer door externe factoren zoals veranderende wet- en regelgeving of wijzigingen in samenwerkingen of technische aspecten zoals wijzigingen in software.
Het verwerkingenregister van de gemeente Enschede bestaat uit ruim 800 processen waarbij het van belang is om bij wijzigingen meteen de juiste acties te ondernemen voor zover deze verband houden met het verwerkingenregister. Deze signalen moeten door de verschillende afdelingen zelf worden doorgegeven.
De aan te stellen AVG-coördinator kan hen hierbij behulpzaam zijn en de helpende hand bieden om het register actueel te houden en relevantie mutaties door te voeren. Daarnaast kan deze ook een signalerende functie vervullen door de afdelingen waar nodig aan te geven dat de mutatie het nodig maakt om de DPIA te herzien.
Een aanvullende aanbeveling die de FG heeft gedaan is om het verwerkingenregister uit te breiden met informatie over of de verwerking DPIA-plichtig is, of de DPIA is uitgevoerd, wanneer deze is uitgevoerd en wanneer de DPIA uiterlijk moet worden gereviewd. Hierbij is het van belang om tijdig een AVG-coördinator aan te stellen om hier voortgang in te kunnen boeken. Risico's zijn op dit moment namelijk onvoldoende in beeld.

AANBEVELING 4

Meer aandacht voor privacy onder medewerkers.

De mens is de belangrijkste schakel in het vertrouwelijk houden van persoonsgegevens en voorkomen van datalekken. Het creëren van meer bewustwording zal sterk bijdragen aan een informatieveilig werken. Een van de manieren waarop dit vormgegeven wordt is middels de campagne veilig werkten. Op dit moment loopt een aanbestedingstraject voor het inkopen van een nieuwe online training van medewerkers. Dit traject verloopt langzaam en het is van belang in 2024 weer een goede nieuwe training beschikbaar te hebben voor zowel nieuwe medewerkers als voor hen die al langer in dienst zijn. Daarnaast is afhankelijk van iemands functie ook specifiekere scholing nodig, bijvoorbeeld ten aanzien van:

- Wanneer een verwerkersovereenkomst moet worden afgesloten en wat daarbij van belang is;
- Welke informatie nodig is voor het opstellen van het verwerkingenregister;
- Waar op gelet moet worden bij het aangaan van samenwerkingsverbanden vanuit AVG perspectief;

- Wanneer informatie wel of niet mag worden gedeeld en welk afwegingskader daarbij kan worden gebruikt;
- Hoe een DPIA uit te voeren en wanneer dit verplicht is.

Bovenstaande zal niet alleen helpen bij de uitvoering van DPIA's, het actueel houden van het verwerkingenregister en het (tijdig) melden van datalekken, maar vooral ook bij het zo veel mogelijk veilig en privacy vriendelijk werken.

AANBEVELING 5

Houdt de aandacht voor DPIA's levendig.

Het is mooi om te zien dat de aandacht voor het uitvoeren van DPIA's in 2023 echt begon te leven. Maar er is meer nodig. Het is nog niet volledig transparant voor welke processen een DPIA verplicht is (hier moet nog een scan voor worden uitgevoerd op alle processen die zijn opgenomen in het verwerkingenregister; zie ook aanbeveling 4) of een DPIA is uitgevoerd, wanneer en waar deze te vinden is. Daarnaast is het van belang om uitgevoerde DPIA's centraal zakelijk te archiveren en deze informatie zo vast te leggen dat hieruit eenvoudig managementinformatie kan worden gegenereerd. Voor processen waarbij een DPIA verplicht is en waar deze (nog) niet is uitgevoerd moet een plan gemaakt worden om hierin alsnog de nodige acties voor uit te zetten. In dit plan moet helder worden of hierbij inderdaad sprake is van een achterstand en in welk tempo en volgens welke prioritering de achterstand weggewerkt kan worden.
Blijf daarbij investeren in scholing over het uitvoeren van DPIA's. In 2023 is gebleken dat hier behoefte aan is en dat scholing helpt om de DPIA kwalitatief goed uit te kunnen voeren. Een mogelijkheid die daarbij onderzocht kan worden is om de scholing in eigen beheer te organiseren zodat tijdens de scholing al gewerkt kan worden aan het uitvoeren van een DPIA binnen de eigen werksetting. De FG beveelt daarbij aan om hier net als in 2023 financiële middelen voor beschikbaar te blijven stellen.
Aangezien veel processen en gebruikte systemen bij gegevens verwerkingen in veel gemeenten identiek zijn wil de Functionaris Gegevensbescherming tevens aanbevelen om hierin samenwerking te zoeken bij andere gemeenten om zo met elkaar het werk lichter te maken maar ook om van elkaar te leren en hierbij met elkaar te kunnen reflecteren.

BIJLAGE 1 - OVERZICHT DPIA'S

Hier volgt een overzicht van de (belangrijkste) DPIA's die in 2023 zijn uitgevoerd of waarmee een begin is gemaakt.

Onderwerp DPIA	Datum	Status
Actieteam	1-11-2023	Afgerond
Anonimiseringssoftware Datamask	2-5-2023	Afgerond
Bodycams	24-2023	Afgerond
Software t.b.v. Or verkiezingen	20-7-2023	Afgerond
Archivering		In behandeling
Bibob in Centric Leefomgeving		In behandeling
Camerabewaking stadhuis		In behandeling
Cameratoezicht milieupleinen		In behandeling
Kennispunt Twente (diverse monitoren): • Twentse Monitor Sociaal Domein (TMSD) • Twentse Onderwijs en Jeugdhulp Monitor (TOJM) • Twentse Monitor Jeugdbeschermingsketen • (TMJK)Monitor Voortijdig Schoolverlaters (VSV)		 Opgeschort Opgeschort Opgeschort Opgeschort
Sociaal Domein: diverse onderwerpen: • W&I - Claimproces • WT - Toegangsproces WMO/Jeugd • Handhaving en Debiteuren - Easy Data Financial search "bankafschriftentool" • PodiumD portaal (vervanging E-suite) • PodiumD Formulieren (vervanging E-suite) • Ondersteuningsproces Toeslagenaffaire • Twentse Belofte • DCW (diverse processen)		 In behandeling In behandeling In behandeling In behandeling In behandeling In behandeling In voorbereiding In voorbereiding
Jongerenaanpak (<23 <27)		In behandeling
IT Platform Twente		In behandeling
Octopus web / digitalisering proces bezwaar en beroep		In behandeling
PgAx; sofware voor : • Maatschappelijke ondersteuning • Tijdelijk huisverbod		 In behandeling In behandeling

• Beschermd wonen • Nazorg gedetineerden		In behandeling In behandeling
Public Roam: Wifi voor gasten		In behandeling
Mijn.enschede.nl		In voorbereiding
Werkplekkensysteem: pré DPIA	20-3-2023	DPIA niet nodig o.b.v. pré-DPIA.
Camera fietstunnels		Project gestopt
Pilot inkomensApp TWI		Afgerond – pilot gestaakt

BIJLAGE 2 - OVERZICHT RECHTEN VAN BETROKKENEN

Mensen hebben een aantal rechten als organisaties zoals gemeente Enschede hun persoonsgegevens verwerken. We noemen dit privacyrechten. Deze rechten zijn bedoeld om mensen controle te laten houden over hun persoonsgegevens. Mensen hebben bijvoorbeeld het recht om te weten wat een organisatie met hun gegevens doet. En ze kunnen organisaties onder meer vragen om inzage in hun gegevens en om hun gegevens te corrigeren of wissen. Zo een vraag noemen we een AVG-verzoek. Hieronder volgt een overzicht van de AVG-verzoeken die de gemeente in 2023 heeft ontvangen. Hierbij moet worden opgemerkt dat, door het nog ontbreken van een centrale registratie, de Functionaris Gegevensbescherming er van uit gaat dat het aantal verzoeken waarschijnlijk hoger is.

	Aantal verzoeken	**Aantal personen die het verzoek betrof**	**Toegekend**	**Afgewezen**	**Ingebrekestelling ontvangen**
Verzoek om inzage	33	64	30	3	13
Verzoek om verwijdering*	4	11	3	0	0
Verzoek om informatie	1	1	1	0	0
AVG klacht	6	8	2	4	0
Totaal	44	94	36	7	13

* Bij één verzoek om verwijdering is na vragen van de gemeente t.b.v. wettelijke controle van de identiteit betrokkene nooit meer wat van deze vrager vernomen.

Toelichting klachten:

Soort klacht	**Reden afwijzing of toekenning**
Gebruik medische gegevens inzake WMO beschikking	Toegewezen. Gegevens waren niet noodzakelijk bij beoordeling toekenning zorg
Gebruik naam betrokkene op factuur	Ongegrond. Niet direct of indirect herleidbaar tot specifieke persoon
Raadpleging BRP	Er heeft geen raadpleging plaatsgevonden, Klacht afgewezen
Gegevens gedeeld met ouder zonder ouderlijk gezag	Terechte klacht. Dossier is aangepast.
Klacht kan niet door klachtencommissie in behandeling worden genomen door op eigen verzoek verwijderen van gegevens	Klacht onterecht. Is gevolg van eigen verwijderverzoek. Uitleg over gegeven.
Klacht t.a.v. doorgeven persoonsgegevens	Kan niet in behandeling worden genomen. Dossier bestaat niet meer i.v.m. verstreken bewaartermijn

BIJLAGE 3 - OVERZICHT DATALEKKEN

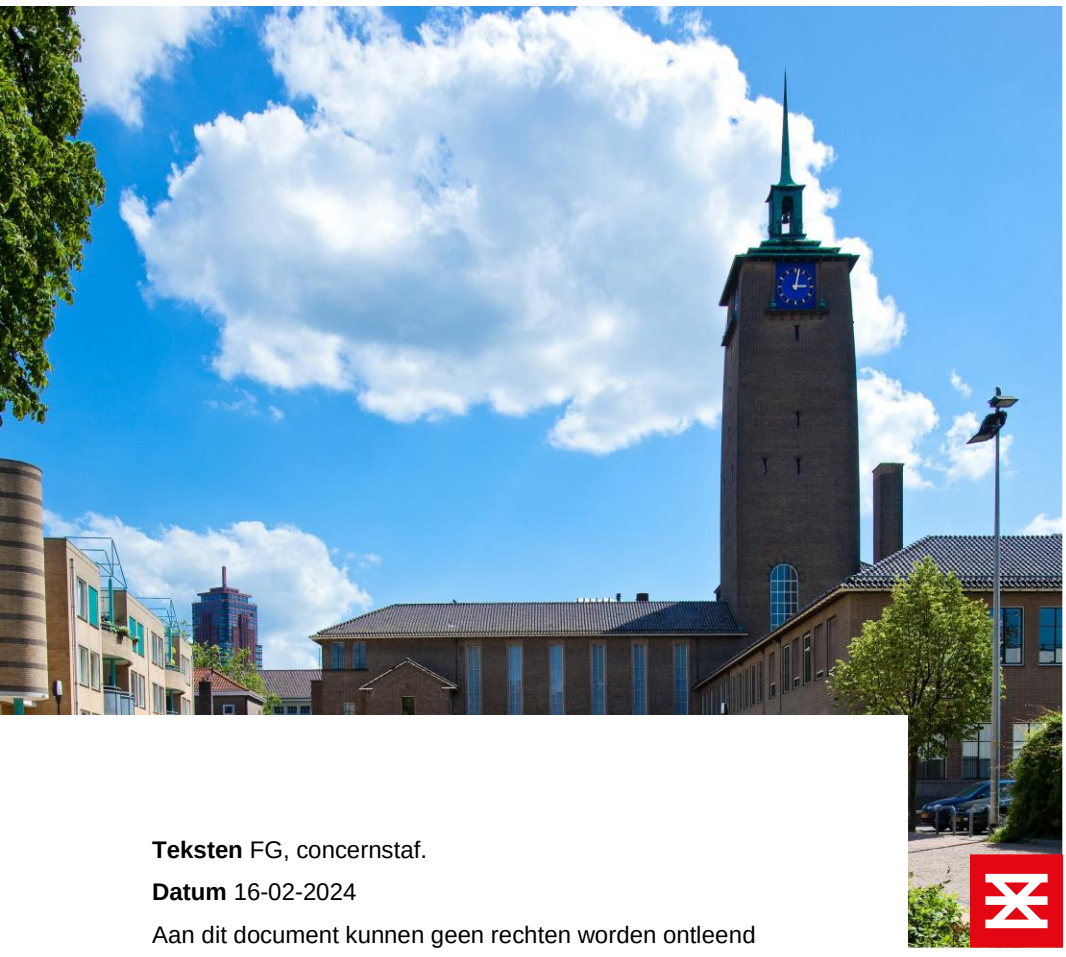
In 2023 zijn in totaal 61 datalekken gemeld. In 2022 waren dit er 56 en in 2021 41. Hieronder volgt een globaal en kort overzicht. Voor het volledige overzicht wordt verwezen naar de separate rapportage datelekken en beveiligingsincidenten over 2023.

Organisatieonderdeel	
Wijkteams	15
Werk en Inkomen	14
Dienstverlening	12
Interne Dienstverlening	9
Omgeving & Recht	7
Ruimtelijke Ontwikkeling & Beheer	2
Beschut	1
Concernstaf	1
Totaal	**61**

Soorten persoonsgegevens	
Algemene persoonsgegevens	56
Bijzondere persoonsgegevens	5
Totaal	**61**

Aard van het incident	
Persoonsgegevens verstuurd of afgegeven aan verkeerde ontvanger	34
Persoonsgegevens per ongeluk gepubliceerd	6
Persoonsgegevens (mondeling) gedeeld met onbevoegde ontvanger	5
Brief of postpakket met persoonsgegevens kwijtgeraakt of geopend retour ontvangen	4
Apparaat, gegevensdrager en/of papier met persoonsgegevens kwijtgeraakt of gestolen	3
Verkeerd dossier gekoppeld in klantportaal	3
Persoonsgegevens mondeling gedeeld met onbevoegde ontvanger	2
Persoonsgegeven van verkeerde klant getoond in klantportaal	1
Persoonsgegevens verstuurd of afgegeven aan verkeerde ontvanger (mail|)	1
Onbevoegde toegang	1
Datalek bij externe verwerker	1
Totaal	**61**

GEMEENTE ENSCHEDE



Teksten FG, concernstaf.

Datum 16-02-2024

Aan dit document kunnen geen rechten worden ontleend

ENSCHEDE