afgewogen

Zwolle

Telefoon

Jaarverslag Functionaris Gegevensbescherming 2024

Verslag voor college en burgemeester

Versie 1.2

Datum 20 mei 2025

Datum	20 mei 2025
Titel	Jaarverslag Functionaris Gegevensbescherming 2024

Datum 20 mei 2025
Titel Jaarverslag Functionaris Gegevensbescherming 2024

Inhoud

2 Managementsamenvatting

2.1 AVG

De bescherming van persoonsgegevens vraagt voortdurende aandacht. Nieuwe wetgeving stelt nieuwe eisen, technologische en maatschappelijke ontwikkelingen leiden tot nieuwe dreigingen en de groei van de gemeentelijke organisatie zorgt ook op het gebied van gegevensbescherming voor uitdagingen.

Om in te kunnen spelen op alle veranderingen hebben organisaties een solide basis nodig. Dit vraagt dit om inzicht in risico's, goede processen om risico's te beperken en vooral ook om medewerkers met voldoende kennis.

De gemeente Zwolle heeft in 2024 stappen gezet om de basis te versterken:

- De in 2023 gestarte bewustzijnscampagne heeft in 2024 geresulteerd in vier opleidingsmodules waarin medewerkers kennis hebben gemaakt met privacy- en informatiebeveiligingsrisico's en hebben geleerd hoe zij daar mee om moeten gaan.
- In 2024 zijn voorbereidingen gestart om een (kwaliteits)managementsysteem te implementeren. Dit moet in 2025/2026 leiden tot een nieuwe manier van werken op basis van een plan-do-check-act-cyclus. Deze kwaliteitsverbetering is in eerste instantie gericht op informatiebeveiligingsprocessen, maar ook voor privacybescherming zal dit positieve impact hebben.
- Het privacyteam is in 2024 versterkt waardoor er meer mogelijkheden zijn gekomen om de organisatie te ondersteunen.
- In 2024 is nieuw privacybeleid vastgesteld.

Voor sommige onderwerpen is echter aanvullende aandacht op korte termijn nodig. Zo heeft de gemeente nog niet voor alle (risicovolle) verwerkingen van persoonsgegevens een zogenaamde data protection impact assessment (DPIA) uitgevoerd. Hierdoor is het zicht van de gemeente op privacyrisico's onvolledig en is dus ook niet zeker dat er voldoende maatregelen getroffen zijn om de persoonsgegevens van inwoners, medewerkers en derden te beschermen.

De informatievoorziening over de bescherming van persoonsgegevens aan inwoners én medewerkers is op dit moment nog niet voldoende. Net als in voorgaande jaren is de borging van privacy bij samenwerkingsverbanden een aandachtspunt. Dit geldt ook voor het zorgen voor tijdige vernietiging van persoonsgegevens.

Ondanks de hierboven genoemde tekortkomingen is duidelijk dat de gemeente Zwolle het onderwerp gegevensbescherming serieus neemt en werkt aan structurele verbeteringen. Dit vraagt ook om een organisatie die bij dit groeipad past. Niet alleen voor de ondersteuning van de organisatie, maar ook voor toezicht dat de organisatie bij de ingezette ontwikkelingen verder helpt. Externe ontwikkelingen, zoals specifieke aandacht van de Autoriteit Persoonsgegevens en autonome professionalisering van de

FG als beroep, maken het eveneens nodig dat de rol en positie van de FG binnen Zwolle versterkt wordt.

2.2 Wpg

In 2024 heeft een interne Wpg-audit plaatsgevonden. Met name op het gebied van DPIA's en IT-ondersteuning zijn er verbeterpunten waaraan in 2025 verder gewerkt wordt. Een belangrijke constatering is verder dat controleprocessen in opzet aanwezig zijn, maar dat documentatie van de uitvoering hiervan ontbreekt. Het is daarmee ook niet aantoonbaar dat de controleprocessen werken. Het ontbreken van vastlegging bemoeilijkt het uitvoeren van audits en toezicht in aanzienlijke mate.

2.3 Ontwikkelingen

Maatschappelijke en technologische ontwikkelingen hebben grote impact op alle organisaties, maar voor gemeenten is die impact groter vanwege de breedte van het takenpakket, de grote waarde van de gemeente voor inwoners, ondernemers en derden, en vanwege de omvangrijke en complexe gemeentelijke informatievoorziening. Landelijke en Europese wetten zorgen voor een betere basis voor de verwerking van persoonsgegevens, geven meer duidelijkheid, maar scheppen tegelijkertijd ook nieuwe verplichtingen waaraan de gemeente moet voldoen. Vanuit privacyperspectief is het belangrijk om zorg te dragen voor tijdige implementatie van nieuwe wetgeving op het gebied van cybersecurity en kunstmatige intelligentie. Ook specifieke privacywetgeving zoals de Wet gegevensverwerking in samenwerkingsverbanden en de Verzamelwet gegevensbescherming vragen in 2025 aandacht.

3 Inleiding

De Algemene Verordening Gegevensbescherming (AVG) schrijft voor dat de functionaris gegevensbescherming (FG) de verwerkingsverantwoordelijke informeert en adviseert over naleving van wet- en regelgeving en beleid op het gebied van de bescherming van persoonsgegevens binnen een organisatie.

Binnen de gemeente geldt het college van B&W als verwerkingsverantwoordelijke voor verwerkingen die worden uitgevoerd in het kader van de gemeentelijke taken aan inwoners, ondernemers, bezoekers en anderen. Ook voor de verwerking van personeelsgegevens is het college verwerkingsverantwoordelijke. Voor een aantal verwerkingen, zoals die met betrekking tot openbare orde en veiligheid, heeft de burgemeester een eigen, zelfstandige verwerkingsverantwoordelijkheid.

De Wet politiegegevens (Wpg) schrijft voor dat de functionaris gegevensbescherming een jaarverslag opstelt met betrekking tot de naleving van de Wpg. Een dergelijk jaarverslag moet worden aangeleverd aan de werkgever van de medewerkers die politiegegevens verwerken (boa’s), namelijk aan het college van B&W.

Met voorliggend jaarverslag rapporteert de FG over de naleving van de AVG en Wpg binnen de gemeente Zwolle, voor zover het verwerkingen betreft die onder verwerkingsverantwoordelijkheid van het college en/of de burgemeester vallen.

Dit jaarverslag is tot stand gekomen op basis van interviews met medewerkers van de gemeente Zwolle (zowel op leidinggevend als op uitvoerend niveau), desk research, inspectie van registers en procesobservatie. Geconstateerde bevindingen en adviezen zijn voorgelegd aan betreffende procesverantwoordelijken. Detailbevindingen, adviezen en reacties zijn integraal meegenomen in de periodieke rapportages aan de directie Zwolle. In voorliggend jaarverslag zijn bevindingen en adviezen op hoofdlijnen beschreven. De organisatie geeft een reactie op deze bevindingen en adviezen in een afzonderlijk document.

3.1 Leeswijzer Jaarverslag

Dit jaarverslag bestaat uit 3 onderdelen:
Deel A betreft het verslag over de AVG;
Deel B gaat in op de Wpg;
Deel C geeft inzicht in relevante ontwikkelingen op het gebied van gegevensbescherming.

In de bijlagen vindt u gedetailleerde informatie over de naleving van de AVG, over de afhandeling van datalekken en over de afhandeling van verzoeken van betrokkenen.

4 Deel A: AVG

4.1 AVG-dashboard

Het AVG-borgingsproduct van VNG (versie 3.0) wordt binnen Zwolle gebruikt om vast te stellen in hoeverre de AVG geïmplementeerd is. Het borgingsproduct onderscheidt zeven hoofdstukken, met per hoofdstuk verschillende paragrafen met specifieke privacyeisen. Hieronder geven wij de score op hoofdstukniveau weer.

§	Titel	2024	2023	Δ
1.	Beleid	50%	40%	↑
2.	Processen	51%	51%	—
3.	Organisatorische inbedding	71%	62%	↑
4.	Rechten van betrokkenen	52%	50%	↑
5.	Samenwerking	33%	33%	—
6.	Gegevensbescherming	63%	61%	↑
7.	Verantwoording	61%	61%	—

Het borgingsproduct van VNG laat zien dat de implementatie van de AVG binnen Zwolle in algemene zin verbetert. De omvang van de verbetering is wel relatief beperkt. Dit betekent dat er nog veel werk verzet moet worden om 100% AVG-compliant te worden.

In de bijlage vindt u de uitgebreide versie van het AVG-dashboard. In de hieronder volgende toelichting geven wij per hoofdstuk inzicht in bevindingen en adviezen.

4.2 Toelichting score AVG-borgingsproduct

4.2.1 Beleid

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

Het privacybeleid is in 2024 opnieuw vastgesteld. De vertaling van het algemene beleid naar specifiek beleid heeft nog in beperkte mate plaatsgevonden. Niet voor alle afdelingen waarbinnen met persoonsgegevens wordt gewerkt bestaan specifieke privacyrichtlijnen. Dit kan leiden tot onrechtmatige verwerkingen van persoonsgegevens en tot handelingsverlegenheid.

De verschillende verantwoordelijkheden voor privacybescherming binnen Zwolse processen zijn in het privacybeleid en in het aanvullende processenboek privacy vastgelegd. Verantwoordelijken zijn echter niet altijd in staat om uitvoering te geven aan de verantwoordelijkheid, vanwege het ontbreken van kennis, middelen en/of voldoende ondersteuning.

In 2025 wordt een inventarisatie uitgevoerd van ontbrekend beleid en zal de FG de organisatie hierover nader adviseren.

4.2.2 Processen

Werkprocessen en DPIA's

De verwerkingen van persoonsgegevens door de gemeente Zwolle moeten voldoen aan de AVG. Dit houdt in dat de gemeente de werkprocessen waarin persoonsgegevens verwerkt worden moet toetsen en inrichten volgens de volgende beginselen: behoorlijkheid, transparantie, doelbinding, dataminimalisatie, opslagbeperking, juistheid, integriteit en vertrouwelijkheid. Daarnaast kan de gemeente in bepaalde gevallen verplicht zijn om een data protection impact assessment (DPIA) uit te voeren. Verder is de gemeente verplicht om alle verwerkingen van persoonsgegevens op te nemen in een register.

In 2024 zijn acht DPIA-trajecten afgerond. Zeven DPIA's betroffen nieuwe verwerkingen. In één geval ging het om een herziening van een eerder uitgevoerde DPIA. Alle DPIA's leidden uiteindelijk tot een positieve advies van de FG over de voorgenomen verwerking.

In 2024 heeft de FG op basis van het onder handen zijnde nieuwe register van verwerkingen een indicatieve toetsing uitgevoerd op het aantal versus vermoedelijk benodigde DPIA's. Hierbij is gekeken naar verschillende risico-indicatoren bij een verwerking van persoonsgegevens, zoals de aard van de verwerkte gegevens en de kwetsbaarheid van betrokkenen. Dit leidde tot de conclusie dat zeer veel DPIA's ontbreken: bij circa 60 verwerkingen is uit de beschrijving van een verwerking af te leiden dat er mogelijk een DPIA, maar toch in ieder geval een initiële toetsing noodzakelijk is. Voor meer dan 40 van deze verwerkingen ontbrak een DPIA geheel en al. Alleen hier blijkt al uit dat de gemeente een grote inhaalslag te maken heeft op het gebied van DPIA's.

In veel gevallen wordt binnen Zwolle een DPIA uitgevoerd vanwege nieuwe of gewijzigde IT of naar aanleiding van een in tijd begrensde activiteit, zoals een project of onderzoek. Dit soort DPIA's zijn zeker nuttig. Maar zolang het gehele proces waarbinnen zo'n activiteit, project of onderzoek wordt uitgevoerd geen onderwerp is geweest van een privacytoetsing levert zo'n in scope beperkte DPIA hooguit een klein venster op alle mogelijke privacyrisico's waarmee rekening moet worden gehouden bij het verwerken van persoonsgegevens.

Ook in het jaarverslag over 2022 en 2023 is geattendeerd op het ontbreken van voldoende DPIA's. Belangrijke oorzaken voor te weinig voortgang op het oplossen van deze bevinding zijn gebrek aan capaciteit en onvoldoende eigenaarschap, al dan niet vanwege onvoldoende kennis en ervaring op het gebied van privacy.

De organisatie is geadviseerd om:

- Het uitvoeren van nu nog ontbrekende DPIA's projectmatig op te pakken om zo de al langer bestaande tekortkoming binnen relatief korte tijd op te lossen.

Bewaren en vernietigen

In 2024 is gestart met het 'bottom-up' verbeteren van informatiebeheer, namelijk door per proces of afdeling knelpunten met betrekking tot informatiebeheer (waaronder ook privacyknelpunten) in kaart te brengen en op te lossen. De voordelen van een dergelijke integrale aanpak zijn duidelijk, maar tegelijkertijd moet worden vastgesteld dat deze aanpak wel meerjarig is. Dit betekent dat de gemeente vermoedelijk nog een aantal jaren niet zal kunnen voldoen aan alle vereisten op het vlak van bewaren en vernietigen van persoonsgegevens.

De organisatie is geadviseerd om:

- Voor risicovolle applicaties een toetsing op tijdige vernietiging uit te voeren en om kaderstellend beleid te formuleren, zodat de grootste risico's versneld kunnen worden opgelost.

4.2.3 Organisatorische inbedding

Privacyteam

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

In 2024 is het privacyteam uitgebreid van 0,7 naar 1,7 FTE. Een dergelijke uitbreiding was noodzakelijk om meer ondersteuning te kunnen bieden aan de organisatie. Deze uitbreiding zorgde er ook voor dat de FG zich vrijwel uitsluitend op zijn eigen taken kon richten, namelijk op toezicht en advies.

Eén van de onderwerpen die in het toezicht over 2024 een belangrijke plek innam is de positionering en rol van de FG zelf. Vastgesteld is dat onvoldoende duidelijk is hoe communicatie- en afstemmingslijnen binnen de ambtelijke organisatie en tussen FG en het bestuur lopen. Ook de huidige organisatorische ophanging van de positie verdient aandacht. Belangrijk om in dit verband op te merken is dat de Autoriteit Persoonsgegevens in 2023 en 2024 verschillende gemeenten kritisch heeft aangesproken op een te zwakke of onjuiste positie van hun FG.

De verdere professionalisering van de gemeentelijke organisatie zal mogelijk vragen om een andere vorm van toezicht door de FG. Duidelijk is ook dat het beroep van functionaris gegevensbescherming, zo'n zeven jaar na de komst van de AVG, toe is aan een autonome professionaliseringsslag. Naar verwachting zullen initiatieven om te komen tot registratie en accreditatie van FG's in 2025 tot concrete uitkomsten leiden. Dit alles maakt het noodzakelijk dat de gemeente Zwolle reflecteert op het benodigde profiel van de FG op middellange termijn.

De organisatie is geadviseerd om:

- De positionering van de FG, het samenspel tussen FG en de ambtelijke organisatie en tussen FG en bestuur vast te stellen en vast te leggen in een regeling FG
- Onderzoek te doen naar het benodigde profiel van de FG op middellange termijn.

Betrokkenheid OR

Er is een vast proces voor het informeren en betrekken van de OR wanneer een nieuwe ontwikkeling impact heeft op de privacy van medewerkers, bijvoorbeeld wanneer sprake is van een systeem waarmee medewerkers gevolgd kunnen worden. Het is niet zeker dat dit in het verleden altijd op dezelfde wijze heeft plaatsgevonden. Een inventarisatie van personeelsvolgsystemen ontbreekt.

De organisatie is geadviseerd om:

- De al voorgenomen inventarisatie van personeelsvolgsystemen af te ronden en voor zover nodig af te stemmen met de OR.

Bewustwording

In 2024 is een bewustwordingscampagne gestart voor informatiebeveiliging en privacy. In vier online modules hebben medewerkers onder meer geleerd over risico's bij het omgaan met persoonsgegevens. De modules gaven medewerkers handvatten om met deze risico's om te gaan.

De bewustzijnscampagne heeft een meer algemeen karakter. Voor een aantal specifieke onderwerpen ontbreken richtlijnen. Bijvoorbeeld voor het goed organiseren van privacy bij samenwerkingsverbanden, voor het verwerken van persoonsgegevens buiten het oorspronkelijke gebruiksdoel en voor het verstrekken van informatie aan derden.

De organisatie is geadviseerd om:

- Voor genoemde onderwerpen specifieke schriftelijke instructies voor medewerkers te formuleren.

4.3 Rechten van betrokkenen

De gemeente dient degene van wie zij de persoonsgegevens verwerkt (betrokkenen) zowel actief als passief te informeren over (de wijze van) het verwerken, de grondslag op grond waarvan dat gebeurt en de maatregelen die de gemeente neemt om onrechtmatige toegang en verwerking te voorkomen. Daarnaast stelt de AVG betrokkenen in staat om middels een aantal 'actieve' rechten controle en invloed uit te oefenen over zijn of haar persoonsgegevens. De gemeente heeft de plicht om de betrokkenen te wijzen op deze rechten en om er voor te zorgen dat de betrokken deze rechten ook daadwerkelijk kunnen uitvoeren.

Recht op informatie

Het recht op informatie is nog onvoldoende geborgd binnen Zwolle. Op de website van Zwolle staat een algemene privacyverklaring en voor een aantal verwerkingen is er een specifieke privacyverklaring. Voor veel van de verwerkingen is echter onvoldoende specifieke informatie beschikbaar.

De organisatie heeft naar aanleiding van eerdere signalen hierover aangegeven dat inwoners geïnformeerd zullen worden over de verwerking van persoonsgegevens via de huidige algemene privacyverklaring, aangevuld met het nog te publiceren register van verwerkingen waarin in detail staat welke gegevens waarvoor worden verwerkt.

Voor wat betreft het informeren van medewerkers heeft de organisatie naar aanleiding van een eerdere rapportage gemeld dat een privacyverklaring voor medewerkers wordt opgesteld.

Beide verbeteracties zijn in 2024 nog niet afgerond.

De organisatie is geadviseerd om:

- De voorgenomen verbeterstappen in 2025 af te ronden, namelijk het afronden van het register van verwerkingen, het publiceren hiervan op de website en het afronden van een privacyverklaring voor medewerkers.

'Actieve' rechten van betrokkenen

De AVG geeft betrokkenen een aantal rechten waar zij zelf een beroep op kunnen doen. Het gaat hier bijvoorbeeld om het recht op inzage, correctie en verwijdering. Binnen Zwolle is hier een goedlopend proces voor ingericht. In bijlage 2 wordt inzicht gegeven in de uitvoering van dit proces in 2024.

Geautomatiseerde individuele besluitvorming

In het jaarverslag over 2023 is vastgesteld dat geen overzicht bestaat van toegepaste geautomatiseerde besluitvorming binnen Zwolle. Geadviseerd werd om aan te sluiten bij de ontwikkelingen met betrekking tot het algoritmeregister, omdat verwacht werd dat daarmee ook inzichtelijk zou zijn waar sprake was van geautomatiseerde besluitvorming. Inmiddels is voorzien in aansluiting op het landelijke algoritmeregister.

Van een inventarisatie van vormen van geautomatiseerde besluitvorming is nog geen sprake geweest.

De organisatie is geadviseerd om:

- De inventarisatie van geautomatiseerde besluitvorming mee te nemen bij de update van het register van verwerkingen.

4.3.1 Samenwerking

Binnen de gemeentelijke context kent samenwerking drie verschijningsvormen. Er kan sprake zijn van opdrachtgeverschap, opdrachtnemerschap of samenwerking in meer letterlijke zin, waarbij partijen voor een gezamenlijk doel of ieder voor een eigen doel samenwerken. Het soort samenwerking én de wijze waarop die samenwerking precies is ingericht bepalen welke taken en verantwoordelijkheden de gemeente heeft ten aanzien van de bescherming van persoonsgegevens.

Wanneer sprake is van opdrachtgever- of opdrachtnemerschap door de gemeente Zwolle zijn er voldoende procedures om te zorgen dat de juiste afspraken gemaakt worden. Centrale vastlegging van gemaakte afspraken ontbreekt echter. Periodieke evaluaties waarin wordt vastgesteld of afspraken worden nageleefd vinden niet altijd plaats. Binnen de Zwolse organisatie zijn verschillende initiatieven onder handen om contractmanagement te versterken.

Vooral waar sprake is van samenwerking in letterlijke zin is het vaak complex om te komen tot goede rolduiding én afspraken. Dit geldt ook voor het verstrekken van informatie aan derde partijen die de gegevens vervolgens zelf voor eigen doelen verwerken. Binnen Zwolle ontbreken heldere beleidsrichtlijnen en instructies hiervoor.

De organisatie is geadviseerd om:

- De informatievoorziening over het aangaan van samenwerkingsverbanden en het verstrekken van informatie te intensiveren, voor zover het privacyaspecten betreft.

4.3.2 Gegevensbescherming

Het niveau van bescherming van persoonsgegevens in 2024 is vergelijkbaar met 2023. Positief is dat gewerkt wordt aan de implementatie van een managementsysteem met een PDCA-cyclus, maar de resultaten hiervan zullen pas in 2025 of 2026 meetbaar zijn. Gelet op de overlap tussen informatiebeveiliging en privacy draagt de implementatie van een managementsysteem voor informatiebeveiliging ook bij aan de versterking van de bescherming van persoonsgegevens.

De organisatie is geadviseerd om:

- Ervoor zorg te dragen dat bij de implementatie van een managementsysteem voor informatiebeveiliging ook vastgelegd wordt hoe dit bijdraagt aan de bescherming van persoonsgegevens, zodat daarmee ook op korte termijn al beter aantoonbaar is hoe de organisatie aan de AVG (en Wpg) voldoet.

4.3.3 Afhandeling datalekken

Het proces voor het afhandelen van privacy-incidenten en datalekken is van een goed niveau, met name daar waar het incidenten met relatief kleine impact betreft. Voor een overzicht van de afhandeling van datalekken in 2024, zie bijlage 3.

4.3.4 Verantwoording

Voor wat betreft verantwoording is het niveau van AVG-implementatie gelijk gebleven. Door de FG wordt periodiek gerapporteerd, maar rapportage en evaluatie vanuit verantwoordelijke afdelingen ontbreekt. Met de implementatie van het managementsysteem met een PDCA-cyclus verwacht de organisatie hier op termijn beter invulling aan te kunnen geven.

5 Deel B: Wpg

5.1 Inleiding

De FG ziet erop toe dat de Wet politiegegevens wordt nageleefd. Het college dient ervoor te zorgen dat de FG naar behoren en tijdig wordt betrokken bij alle gelegenheden die verband houden met de bescherming van politiegegevens. De FG rapporteert jaarlijks de bevindingen aan de hand van een jaarverslag.

In dit jaarverslag staat beschreven welke acties en maatregelen in 2024 zijn genomen om de doelstellingen en beginselen uit de Wet politiegegevens (Wpg) te behalen en te waarborgen. Binnen Zwolle is de Wpg van toepassing op de boa-taakgebieden toezicht en handhaving in de openbare ruimte, leerplicht en sociale recherche.

5.2 Bevindingen en aanbevelingen 2024

De Wpg schrijft voor dat iedere vier jaar een externe audit en ieder jaar een interne audit moet plaatsvinden. Uit de externe audit van 2022 bleek dat de gemeente Zwolle, net als veel andere gemeenten overigens, de naleving van de uit de Wpg-voortkomende verplichtingen onvoldoende kon aantonen. Een heraudit binnen één jaar was daarom noodzakelijk.

Na de audit is een externe Wpg-coördinator aangesteld om het verbetertraject richting heraudit te begeleiden. De doelstelling voor de heraudit was om voor 80% te voldoen aan alle vereisten, waarna een jaar later 100% naleving moest zijn bereikt. In mei 2023 vond de heraudit plaats.

De heraudit toonde aan dat er veel vooruitgang is geboekt binnen alle domeinen. De doelstelling voor de heraudit (80% naleving) was behaald. De relatief grootste nog bestaande verbeterpunten betroffen IT-beheersing, interne controle en audit en toezicht.

In 2025 heeft een interne audit plaatsgevonden die zich richtte op die zaken die tijdens de externe audit nog niet op orde waren bevonden. De interne audit liet wederom verbeteringen zien. Zo worden de mogelijkheden om de IT-ondersteuning te laten aansluiten bij alle vereisten van de Wpg onderzocht. De actiepunten zijn nog niet afgerond. Verder is vastgesteld dat voor alle domeinen een DPIA aanwezig is, maar dat deze niet in alle gevallen volledig is. Ook plannen met betrekking tot audit en toezicht waren onvoldoende actueel. Daarmee is dus nog geen sprake van 100% naleving.

Voor alle openstaande bevindingen zijn acties in 2025 gepland. De mate van naleving zal opnieuw getoetst worden via een externe audit, die in de tweede helft van 2025 zal plaatsvinden.

Het toezicht op de Wpg door de FG bestond in 2025 primair uit documentonderzoek, bijdragen aan en reviewen van de interne audit en het voeren van periodieke voortgangsgesprekken met de verschillende domeinen. In aanvulling op de bevindingen

uit de interne audit is daarbij vastgesteld dat controleprocessen in opzet aanwezig zijn, maar dat controles nog niet aantoonbaar worden uitgevoerd. Dat maakt het uitvoeren van gedetailleerd toezicht lastig of in sommige gevallen zelfs onmogelijk. Het gaat hier bijvoorbeeld om het toezicht op verstrekkingen van politiegegevens. De organisatie is zich bewust van het belang van adequate documentatie van uitgevoerde controles. Bij de volgende toetsing van naleving zal de voortgang opnieuw worden gemeten.

De Wpg schrijft voor dat er – binnen strikte kaders – sprake moet zijn van gegevensuitwisseling binnen het politiedomein. Samen met twee andere gemeenten en de politie zijn in 2024 verkenningen gestart om die gegevensuitwisseling te optimaliseren conform Wpg-vereisten.

6 Deel C: Ontwikkelingen: IT en wetgeving

6.1 Cybersecuritywet

Onze grote afhankelijkheid van IT en de toename van cyberrisico's vragen om een hoog niveau van informatiebeveiliging. De snelle ontwikkeling van AI en van superkrachtige computers maakt dat de uitdagingen voor informatiebeveiligers groter zijn dan ooit. Organisaties moeten kunnen inspelen op snelle technologische ontwikkelingen. Dit vraagt om voldoende specialistische kennis én volwassen risicomanagement.

De Europese Raad heeft in 2022 de NIS2-richtlijn vastgesteld. Met deze richtlijn worden EU-lidstaten gedwongen om op onderling vergelijkbare wijze informatiebeveiligingswetgeving te implementeren. Binnen Nederland gebeurt dit met de Cyberbeveiligingswet die naar verwachting in 2025 in werking zal treden.

Voor gemeenten betekent dit dat zij een wettelijke zorgplicht krijgen voor digitale veiligheid. Gemeenten worden verplicht om te voldoen aan de Baseline Informatiebeveiliging Overheid 2 (BIO2). Deze norm is vooral gericht op de organisatie van informatiebeveiliging en op goed functionerend risicomanagement. Daarnaast schrijft de norm een aantal specifieke beveiligingsmaatregelen voor de overheid voor.

De gemeente Zwolle richt zich bij de inrichting van een PDCA-cyclus voor informatiebeveiliging als eerste op het implementeren van cybersecuritywetgeving.

6.2 Wet gegevensverwerking in samenwerkingsverbanden

Op 1 maart 2025 is de Wet gegevensverwerking in samenwerkingsverbanden (Wgs) in werking getreden. Deze wet regelt de gegevensverwerking binnen vier specifieke domeinen. Twee hiervan zijn ook relevant binnen Zwolle, namelijk de regionale samenwerking binnen het Regionale Informatie- en Expertisecentrum en de samenwerking binnen het Zorg- en Veiligheidshuis IJsselland.

De Wgs leidt tot nieuwe afspraken met partners en nieuwe verplichtingen, waaronder het benoemen van een coördinerend FG voor de samenwerkende partijen, het instellen van een centraal contactpunt voor betrokkenen en het laten uitvoeren van audits. Voor het Zorg- en Veiligheidshuis geldt dat Zwolle een voortrekkersrol heeft bij het implementeren van de nieuwe wetgeving – het Zorg- en Veiligheidshuis is immers gepositioneerd binnen de Zwolse ambtelijke organisatie.

6.3 Wet gegevensverwerking persoonsgerichte aanpak radicalisering en terroristische activiteiten (Wet PARTA)

De Wet PARTA is op 28 januari aangenomen door de Eerste Kamer. Met deze wet krijgen burgemeesters de wettelijke taak om casusoverleggen te organiseren gericht op het de aanpak van radicaliserende of geradicaliseerde personen. Met de wet wordt de juridische basis voor een veelal reeds bestaande praktijk versterkt. De wet zorgt voor duidelijkheid over gegevensuitwisseling tussen deelnemers aan een casusoverleg. Net

als de Wgs schrijft ook de Wet PARTA voor dat een coördinerend FG wordt aangewezen, een contactpunt voor betrokkenen wordt ingesteld en periodieke privacyaudits worden uitgevoerd. De wet zal naar verwachting medio 2025 in werking treden.

6.4 AI-verordening

Sinds de komst van ChatGPT in 2022 is AI in het middelpunt van de publieke belangstelling komen te staan. Naast taalmodellen zoals ChatGPT zijn ook verschillende systemen beschikbaar gekomen om gemakkelijk beelden te creëren of te manipuleren. Dit heeft geleid tot veel optimisme over de mogelijkheden van kunstmatige intelligentie, maar ook tot minstens evenveel zorgen over de risico's van deze nieuwe technologie voor de mens.

Vanaf 2018 heeft de Europese Commissie een voorstel voor het reguleren van AI in voorbereiding. Doel hiervan was het versterken van de positie van de EU bij de ontwikkeling van AI én het zorgdragen dat AI ten dienste van de mens en de samenleving komt. Op 1 augustus 2024 is het uiteindelijke commissievoorstel in werking getreden: de AI-verordening.

De AI-verordening maakt onderscheid tussen verschillende risiconiveaus voor AI-systemen en geeft dwingende voorschriften voor elk van deze niveaus. Systemen met een onacceptabel risico zijn verboden, voor systemen met een hoog of beperkt risico gelden voorwaarden, en systemen met een minimaal risico worden niet gereguleerd. Voor zogenaamde 'general purpose AI', zoals ChatGPT en CoPilot, zijn afzonderlijke regels vastgesteld.

De AI-act geldt niet alleen voor aanbieders van AI, maar ook voor importeurs en distributeurs, organisaties die AI gebruiken en voor fabrikanten die AI in hun producten gebruiken.

De bepalingen van de AI-verordening zijn niet allemaal direct van toepassing. Vanaf februari 2025 zijn verschillende AI-systemen, zoals systemen die mensen manipuleren of misleiden, verboden. Ook zijn werkgevers verplicht om medewerkers AI-geletterd te maken, zodat iedereen gelijkelijk kan profiteren van de mogelijkheden van AI. In augustus 2025 zullen eisen voor 'general purpose AI' in werking treden. Vanaf 2026 zullen stapsgewijs ook de regels voor AI-systemen met een hoog risico van toepassing worden.

De AI-act betekent voor organisaties allereerst dat zij inzichtelijk moeten hebben welke vormen van AI zij gebruiken. Hier moeten organisaties transparant over zijn. Organisaties moeten een volwassen niveau van risicomanagement en informatiebeveiliging hebben om te zorgen dat het gebruik van AI verantwoord plaatsvindt.

6.5 Verzamelwet gegevensbescherming

De Verzamelwet gegevensbescherming is in behandeling bij de Tweede Kamer. Met deze wet wordt de Uitvoeringswet AVG (UAVG) gewijzigd. De verzamelwet zorgt voor een betere juridische basis voor het gebruik van persoonsgegevens door accountants, versterkt de privacyrechten van jongeren en geeft meer duidelijkheid over de (on)mogelijkheden voor het gebruik van biometrische gegevens. De datum van inwerkingtreding van de wet is nog onbekend.

7 Bijlage 1: Gedetailleerd AVG-dashboard

§	Titel	2024	2023	Toelichting 2024
1.	Beleid	50%	40%	Het privacybeleid is in 2024 vastgesteld. Dit beleid vormt een algemeen kader. De vertaling van het algemene beleid naar specifiek beleid is nog niet in alle gevallen aanwezig. Verantwoordelijkheden voor het borgen van privacy zijn in het privacybeleid en in het aanvullende processenboek privacy vastgelegd. Verantwoordelijkheden zijn niet altijd in staat om uitvoering te geven aan de verantwoordelijkheid, vanwege het ontbreken van kennis, middelen en/of ondersteuning.
1.2	Privacybeleid	53%	0%	
1.3	Verantwoordelijkheden	46%	50%	
2.	Processen	51%	51%	In 2024 is een update van het register van verwerkingen gestart, maar niet voltooid. Niet voor alle verwerkingen is een DPIA uitgevoerd. Dit vormt een compliancerisico voor de gemeente. Belangrijker is echter dat hierdoor onvoldoende zicht is op risico's voor inwoners, medewerkers en anderen. In 2024 is gestart met het verbeteren van bewaar- en vernietigingsbeleid. Gelet op de omvang van de opgave is te verwachten dat het volledig voldoen aan wettelijke vereisten pas over enkele jaren haalbaar zal zijn.
2.1	Werkprocessen	45%	38%	
2.2	Verwerkingsregister	73%	83%	
2.3	Pre-DPIA's	33%	13%	
2.4	DPIA's	55%	55%	
2.5	Bewaar- en vernietigingsbeleid	28%	25%	
3.	Organisatorische inbedding	71%	62%	Het privacyteam is in 2024 versterkt. Gelet op interne en externe ontwikkelingen is het van belang om rol en positionering van de FG opnieuw te overwegen en vast te stellen. De voorgenomen verbetering van het betrekken van de OR bij personeelsvolgsystemen is in 2024 niet uitgevoerd. Het alsnog uitvoeren hiervan is voor 2025 gepland.
3.1	Privacyteam	75%	13%	
3.2	Aanstelling, positie en taken FG	73%	83%	
3.3	Informeren OR	63%	63%	
3.4	Bewustwording	70%	40%	
4.	Rechten van betrokkenen	52%	50%	De afhandeling van verzoeken van betrokken is van een goed niveau. Het informeren over verwerkingen die de gemeente uitvoert is nog onvoldoende. Voor 2025 zijn verbetermaatregelen gepland. De komst van het algoritmeregister is aanleiding geweest voor meer aandacht voor geautomatiseerde individuele besluitvorming. Risico's op dit punt blijven echter significant, ook door de onverminderd sterke ontwikkeling van AI.
4.1	Recht op informatie	30%	33%	
4.2	Processen rechten van betrokkenen	86%	88%	
4.3	Toestemming	38%	38%	
4.4	Geautomatiseerde individuele besluitvorming	31%	8%	
4.5	Websites en applicaties	58%	50%	
4.6	Technische ondersteuning	31%	31%	
5.	Samenwerking	33%	33%	Risico's in de keten zijn omvangrijk. Formele relaties bij samenwerkingen zijn vaak niet duidelijk, en daarmee is niet helder wat de basis is voor gegevensuitwisseling. Ook op het gebied van incidentele gegevensverstrekkingen ontbreekt overzicht en inzicht in rechtmatigheid. Geplande maatregelen zien met name op het verbeteren van de informatievoorziening.
5.1	AVG rollen	47%	50%	
5.2	Gegevensverstrekking	18%	18%	
6.	Gegevensbescherming	63%	61%	Het niveau van bescherming van persoonsgegevens in 2024 is vergelijkbaar met 2023. Positief is dat gewerkt wordt aan de implementatie van een managementsysteem met ene PDCA-cyclus, maar de resultaten hiervan zullen pas in 2025 of 2026 meetbaar zijn. Het proces 'afhandelen privacy-incidenten en datalekken' is van een goed niveau, met name daar waar het incidenten met relatief kleine impact betreft.
6.1	Risico's	50%	50%	
6.2	Gegevensbescherming door ontwerp	63%	63%	
6.3	Gegevensbescherming door standaardinstellin	50%	50%	
6.4	Informatiebeveiliging	55%	53%	
6.5	Privacyincidenten en datalekken	73%	69%	
7.	Verantwoording	61%	61%	Voor wat betreft verantwoording is het niveau gelijk gebleven. Door de FG wordt periodiek gerapporteerd, maar rapportage en evaluatie binnen verantwoordelijke afdelingen ontbreekt. Met de implementatie van het managementsysteem met een PDCA-cyclus wordt verwacht hier op termijn invulling aan te kunnen geven.
7.1	Evaluatie naleving AVG	56%	56%	
7.2	Evaluatie informatiebeveiliging	50%	50%	
7.3	Rapportage	100%	100%	

Datum 20 mei 2025

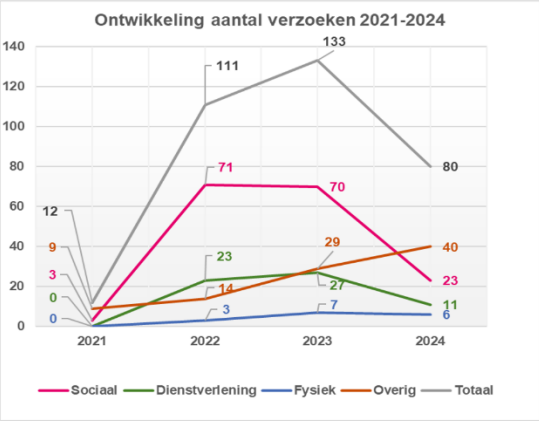
Titel Jaarverslag Functionaris Gegevensbescherming 2024

8 Bijlage 2: Rapportage verzoeken betrokkenen 2024

Inleiding
Op grond van artikel 15-21 AVG hebben betrokkenen het recht op inzage, rectificatie/aanvulling, gegevenswissing, beperking van de verwerking op overdraagbaarheid van de verwerkte gegevens en het recht van bezwaar tegen een verwerking. Doel van deze rechten is om betrokkenen in staat te stellen controle te houden over de verwerking van persoonsgegevens. De Wpg geeft een betrokkene soortgelijke rechten voor wat betreft de verwerking van politiegegevens (art. 25, 28 Wpg).

AVG- en Wpg-verzoeken kunnen worden ingediend via Mijn Loket, of per mail/post. Op de afhandeling is de Algemene wet bestuursrecht van toepassing. Een besluit om een verzoek in te willigen is dan ook een besluit in de zin van de Awb, waartegen bezwaar kan worden gemaakt.

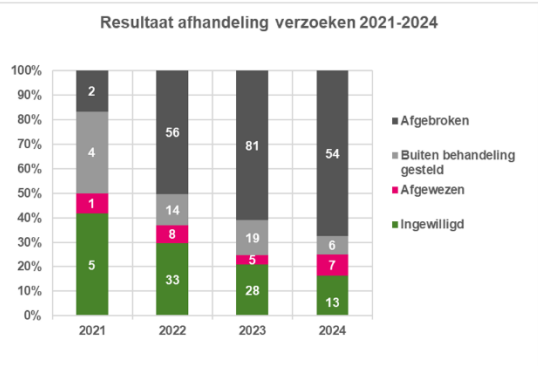
Voorliggende rapportage betreft de binnen Zwolle afgehandelde verzoeken van betrokkenen over 2024.



In deze rapportage wordt onderscheid gemaakt tussen vier domeinen binnen Zwolle: sociaal, dienstverlening, fysiek en overig. Bij verzoeken in domein 'overig' gaat het bijvoorbeeld om verzoeken die meerdere domeinen betreffen, onduidelijke verzoeken die niet door indiener zijn aangevuld/toegelicht en om verzoeken die bij de gemeente Zwolle zijn ingediend, maar niet de Zwolse organisatie betroffen. Denk bijvoorbeeld aan verzoeken met betrekking tot informatie die bij GBLT berust.

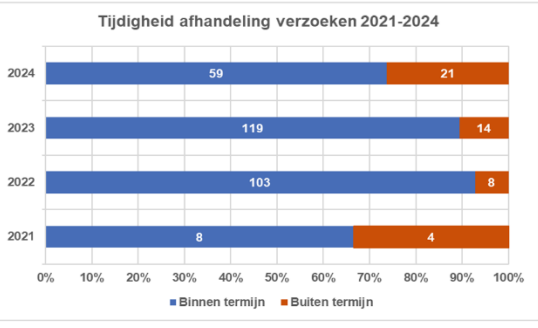
Ten opzichte van 2023 is het aantal verzoeken sterk gedaald, namelijk van 133 naar 80 (-40%). Een direct aanwijsbare oorzaak hiervoor is een technische aanpassing op de website. In 2022 en 2023 zijn relatief veel verzoeken ontvangen van personen die op de website ten onrechte waren geleid naar het formulier waarmee ze een verzoek konden indienen. In 2024 is het formulier waarmee je verzoeken kan indienen heringericht.

In 2024 hadden 3 verzoeken betrekking op de Wpg, 70 op de AVG en in 7 gevallen was dit onduidelijk of betrof het geen verzoek op grond van de AVG of Wpg.



Ondanks dat er in 2024 minder onbedoelde verzoeken zijn ontvangen dan in 2023 is het percentage verzoeken dat niet inhoudelijk behandeld is gelijk gebleven: 75%. In deze gevallen gaat het om verzoeken die onvolledig waren en niet (tijdig) zijn aangevuld, om verzoeken die zijn ingetrokken en om verzoeken die bij nadere beschouwing niet kwalificeerden als verzoek op grond van de AVG of Wpg, maar bijvoorbeeld als Woo-verzoek.

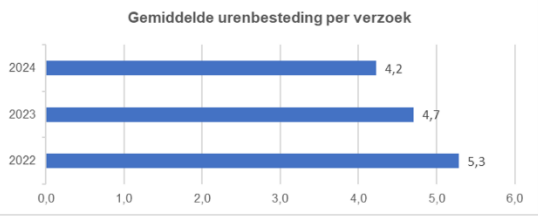
Van de verzoeken die inhoudelijk zijn behandeld zijn er 13 ingewilligd en 7 afgewezen. Dit betekent dat van alle verzoeken die zijn ontvangen slechts 16% resulteerde in een toekenning. Dit betekent niet dat alleen in die gevallen een verzoeker de informatie ontving waar hij/zij op zoek naar was - het is mogelijk dat een verzoeker informatie heeft gevonden buiten de context van het AVG-/Wpg-verzoek, maar dit is niet met zekerheid te stellen.



In 2024 zijn 59 van de 80 verzoeken tijdig afgehandeld, dat wil zeggen: 74%. In 2022 en 2023 was dit nog 94% en 89%. Voor deze afname zijn twee oorzaken aan te wijzen:

1) In de periode januari-september 2024 was de beschikbare personele capaciteit voor het afhandelen van verzoeken kleiner dan in 2022 en 2023.

2) In Q1/Q2 zijn verschillende verzoeken in behandeling genomen door externe inhuur. Deze inzet voldeed niet aan onze kwaliteitsstandaarden waardoor de afhandeling van deze verzoeken moest worden overgenomen en pas in Q3 afgerond is. Betreffende inhuur is inmiddels beëindigd.



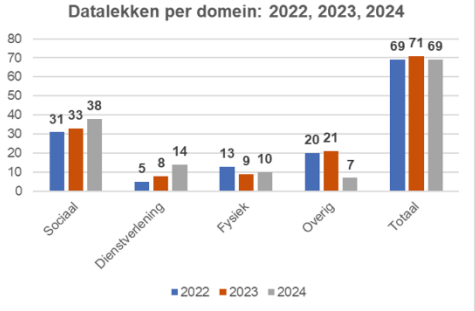
De gemiddelde urenbesteding is in 2024 verder gedaald, namelijk naar 4,2 uur per verzoek. De totale urenbesteding is in 2024 gedaald van 626 naar 338 uur.

9 Bijlage 3: Rapportage datalekken 2024

Inleiding
'Datalek' is de veelgebruikte term voor 'inbreuk in verband met persoonsgegevens'. Artikel 4 lid 12 AVG geeft de volgende definitie: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.'

Een dergelijke inbreuk moet gemeld worden aan de Autoriteit persoonsgegevens (AP) 'tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen' (art. 33 lid 1 AVG). De Wpg kent soortgelijke bepalingen (art. 33a Wpg). Als de inbreuk een hoog risico vormt voor degene van wie gegevens zijn gelekt, dan moet deze betrokkene op de hoogte gesteld worden van het datalek.

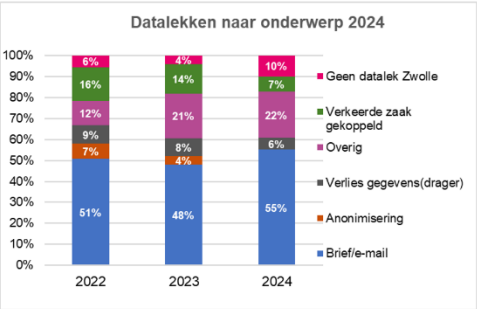
Voorliggende rapportage gaat over de binnen Zwolle geregistreerde datalekken over 2024.



In deze rapportage maken we verschil tussen vier domeinen binnen Zwolle: sociaal, dienstverlening, fysiek en overig. Bij datalekken in domein 'overig' gaat het bijvoorbeeld om datalekken die te maken hebben met de interne organisatie (bijvoorbeeld mails die verstuurd zijn aan een verkeerde medewerker) of om binnen Zwolle gemelde datalekken die geen betrekking hadden op Zwolle, maar een andere organisatie (bv. een partner of leverancier). Eén van dit soort datalekken in 2024 had betrekking op de griffie.

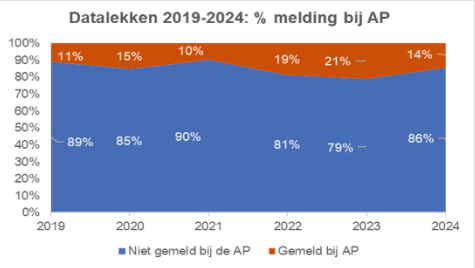
Het aantal gemelde datalekken in 2024 lag 3% hoger dan in dezelfde periode in 2023. Alle datalekken hadden betrekking op een AVG-gegevensverwerking.

Opvallend is de stijging van het aantal datalekken binnen het domein dienstverlening. Hiervoor is niet direct een inhoudelijke oorzaak aan te wijzen.



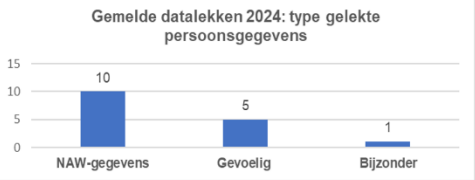
Net als in voorgaande jaren hebben relatief veel datalekken te maken met het gebruik van e-mail. Twee typen laten zich onderscheiden:
1) mails gestuurd naar een verkeerde ontvanger
2) mails gestuurd naar de juiste ontvanger, maar in de mail staan persoonsgegevens van een derde (bv e-mailadressen).

Het aantal keren dat een gemeld incident geen datalek voor Zwolle betrof is relatief sterk toegenomen. Het gaat hier bijvoorbeeld om datalekken die door Zwolle zijn opgemerkt, maar waarvoor Zwolle niet verantwoordelijk is. Het kan hier gaan over een datalek betreffende een gegevensverwerking die Zwolle namens een andere gemeente uitvoert. In dat geval is de andere gemeente verantwoordelijk voor het beoordelen en eventueel melden van het datalek. Een van dergelijke datalekken heeft geleid tot afstemming tussen privacy officers van Zwolle en andere gemeenten voor het versterken van de afspraken over de omgang met dit soort datalekken.

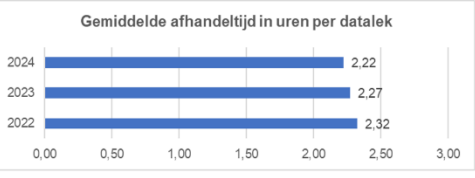


Opvallend is de daling van het percentage datalekken dat gemeld is bij de AP. Dit hangt ook samen met de toename van het aantal incidenten dat niet kwalificeert als datalek, of niet als datalek waarvoor Zwolle verantwoordelijk is.

In totaal zijn tien datalekken bij de AP gemeld. In negen gevallen ging het om datalekken die verband hielden met het beschikbaar komen van persoonsgegevens voor een onbevoegde (vooral vanwege fouten met mailverzending). Zeven van deze datalekken zijn gemeld vanwege een verhoogd risico voor betrokkene. Het tiende gemelde datalek betrof het zoekraken van een lijst met namen. Betrokkenen zijn niet geïnformeerd omdat het risico voor betrokkenen als beperkt werd geschat.



Bij de gemelde datalekken ging het in alle gevallen om 'reguliere' persoonsgegevens zoals naam, adres, contactgegevens en geslacht. In vijf gevallen ging het om persoonsgegevens van gevoelige aard, zoals BSN en financiële gegevens. Eénmaal betrof het bijzondere persoonsgegevens, namelijk gegevens van medische aard.



De gemiddelde netto ***afhandeltijd*** per datalek is min of meer gelijk aan vorige jaren.

Indien sprake is van een meldingsplichtig datalek moet sprake zijn van een maximale ***doorloop*** tot aan de melding bij de AP van 72 uur. De huidige administratie van datalekken in Topdesk geeft hier geen sluitende informatie over. In 2025 wordt onderzocht hoe we de administratie op dit punt kunnen verbeteren.