Jaarrapportage privacy 2024

[redacted]
Functionaris voor de Gegevensbescherming (FG) gemeente Nijmegen
Stadscontrol

e-mail: Functionarisgegevensbescherming@nijmegen.nl

Versie 1 24/04/25/PK

Inhoudsopgave

Inhoudsopgave 1

Management samenvatting 2

1. Inleiding 3

2. Stand van zaken privacy binnen de gemeentelijke organisatie 4
2.1 Quick scan Privacy 4
2.2 VNG AVG Borgingsproduct 3.0 jaar 2024 6
2.3 Rapportage rekenkameronderzoek informatiebeveiliging en privacy 7

3. Uitvoering Privacy beleid 8
3.1 Privacy beleid update 8
3.2 Rechten van betrokkenen 8
3.3. Incidenten en Datalekmeldingen 8
3.4. Afhandeling Klachten 8
3.5. Onderzoek door of namens de FG, postbus FG 8

4. Check op de naleving op basis van interne controle 2024. 9
4.1. Uitvoering van de plannen van aanpak ‘Mijn afdeling privacy proof’ 9
4.2. Wpg Audit 10
4.3. DPIA als continu bijstuurproces 11
4.4. Register van Verwerkingen 12
4.5. Tafel van Elf 13
4.6. Privacy Protocollen 14
4.7. Archivering / vernietiging 14

5. Bewustwording en weerbaarheid 15
5.1. Vergroting I-bewustzijn 15
5.2. Privacy Ambassadeurs 15

6. Conclusies 16

Bijlagen 17
1. Tabel Scores Interne Audit 18
2. Tabel stand van zaken uitgevoerde DPIA’s 19
3. Duiding ‘Volwassenheidsniveau 3’ 20
4. Duiding gebruikte afkortingen 21

Management samenvatting

In 2024 heeft de organisatie van de gemeente Nijmegen wederom goede stappen voorwaarts gezet. Maar als FG moet ik ook constateren dat we er nog zeker niet zijn. En dat dit ook niet vanzelf goed komt.
Afgelopen jaar zijn er weer een aantal substantiële vorderingen gemaakt: eindelijk is het project 'Mijn Afdeling AVG proof' afgerond. De laatste afdeling (IZL) heeft zijn projectplannen ingediend. Let wel: nu zijn pas de voorwaarden om te komen tot een 'AVG-proof' organisatie ingevuld. Dat wil nog niet zeggen dat de organisatie AVG-proof is.
Ik heb dit, net als vorig jaar, weergegeven in een stoplichten model: rood, geel en groen. Deze kleuring is een eerste stap naar het weergeven van kritische prestatie indicatoren (KPI's) op het domein van privacy.

Waar langzaam de opzet en het bestaan van maatregelen en activiteiten is ingevuld, komt het nu aan om te laten zien dat de werking van naleving van de AVG functioneert. Daarmee wordt de lat hoger gelegd en kunnen de kleuren op dát hogere niveau alsnog geel of soms rood geven. De organisatie wil toegroeien naar een beheerniveau 3 (uitleg zie bijlage) en daar past deze toetsing bij. Dat is een stap voorwaarts in de ontwikkelfase.

Ondanks deze stappen in de goede richting, resteert nog steeds een harde constatering: AVG-proof op de volle breedte is de organisatie nog niet. Problemen, die nog opgelost moeten worden, zijn hardnekkig. Invoeren van de nieuwe werkwijze - *dataminimalisatie is nu het uitgangspunt* – wordt vormgegeven. Dit betreft acceptatie en internalisering bij medewerkers, maar ook aanpassen van allerlei processen en procedures. Vanaf 2023 zijn hier extra middelen voor vrij gemaakt. Dit vergt nog een forse inspanning in de organisatie.

Het opstellen van een risicoscan (in de vorm van DPIA's) is nog steeds groeiende. Het naleven van de maatregelen zoals opgenomen in de DPIA's is langzaam de standaard aan het worden. Evidenced based aanleveren (aantoonbaar laten zien dat het werkt zoals afgesproken) is groeiende, maar is nog geen gemeengoed.
Het is wél de lijn die ik uitdraag als FG.
In 2024 zijn er 31 DPIA's opgesteld en voorzien van advies door de FG. De organisatie kent een sluitende procedure voor wat betreft het opstellen van DPIA's bij nieuwe processen, aanschaf applicaties voor bestaande processen en nieuwe wetgeving. In 2024 is de achterstand op belangrijke processen verder ingelopen. De VNG heeft een lijst "Must Have DPIA's' gepubliceerd. Van de genoemde processen waarvan een DPIA wordt aangeraden, heeft de organisatie het merendeel afgerond en van een deel is het proces gestart om tot een privacy scan te komen. Afronding hiervan wordt in 2025 verwacht.
Naleving van verwerkersovereenkomsten is matig tot slecht. Hier scoort de organisatie nog onvoldoende.
In 2024 zijn er verdere stappen gezet op het gebied van privacy protocollen (en de naleving hiervan) voor allerlei samenwerkingsverbanden. Het maken van een overzicht is gestart in 2024 en wordt afgerond in 2025.

Tenslotte zijn er stappen gezet om de bewustwording en weerbaarheid in de organisatie te vergroten: medewerkers dienen verplichte leerlijnen privacy en informatiebeveiliging te volgen. Acceptatie en voldoende kennis en kunde blijft echter een grote uitdaging binnen de organisatie van de gemeente Nijmegen.

[redacted]
Functionaris voor de Gegevensbescherming Nijmegen
24 April 2025

1. Inleiding

Deze jaarrapportage maakt onderdeel uit van de wettelijke verantwoordingsplicht vanuit de AVG-wetgeving. De jaarrapportage is gemaakt door de FG van de gemeente Nijmegen. De meest relevante punten zijn opgenomen in de paragraaf 'privacy maatregelen' in het (verplichte) ENSIA verantwoordingstraject.

Dit jaarverslag is mede tot stand gekomen door inbreng van de Privacy Officer en de Privacy adviseurs. Daarnaast heb ik dankbaar gebruik gemaakt van andere waardevolle reflecties. Ik heb wederom gebruik gemaakt van het format van vorig jaar. Ik kan nu op onderdelen laten zien wat de verschillen zijn tussen 2022, 2023 en 2024. Zo ontstaat er langzaam een tijdlijn en na een aantal jaren wellicht een trend.

Dit jaarverslag richt zich op de gemeentelijke organisatie. Dat betekent dat de relatie en bereikte resultaten van de FG met (het presidium van) de Raad, het College, de Griffie (eigen traject van AVG-proof) en de Rekenkamer (idem met een goede eigen aanpak) hierin níet opgenomen zijn.

De gemeentesecretaris zal als de eindverantwoordelijke binnen de organisatie van de gemeente Nijmegen deze jaarrapportage ontvangen. Tevens wordt de rapportage besproken met de betrokken bestuurders: de portefeuillehouder Digitalisering en de Burgemeester.

Leeswijzer

- In het volgende hoofdstuk (H2) ga ik dieper in op de 'stand van zaken met betrekking tot de privacybescherming' binnen de organisatie van de gemeente Nijmegen. Dit gebeurt zowel kwalitatief (in de vorm van een quick scan) als kwantitatief (in de vorm van een interne audit, die zowel kwalitatief als kwantitatief is). Beiden betreffen een 'overall view'.
  Tevens meld ik de vorderingen op de aanbevelingen van het onderzoek dat de Rekenkamer Nijmegen heeft uitgevoerd naar de informatiebeveiliging en privacybescherming binnen de gemeente Nijmegen.
- Met hoofdstuk 3 ga ik nóg verder de diepte in en verken ik de (jaarlijkse update van de) stand van zaken van de uitvoering van het privacy beleid. Deze vormt de basis van de jaarlijkse control door de FG op de uitvoering en naleving hiervan.
- De resultaten hiervan vinden haar weerslag in hoofdstuk 4: Check op de naleving op basis van interne control 2024.
- In detail ga ik vervolgens in op de voortgang van diverse projecten, de uitkomsten van de verplichte audit op de Wpg (Wet politie gegevens), de uitvoering van het instrument DPIA (Data Protection Impact Assesment), naleving verwerkersovereenkomsten, uitvoering privacy protocollen en de maatregelen om het I-bewustzijn binnen de organisatie te vergroten (hoofdstuk 5).
- Tenslotte staan in de bijlagen de (detail)uitkomsten van de interne audit, de stand van de DPIA's per 31 december 2024, de duiding van het gebruikte 'Volwassenheidsniveau 3' als beheerorganisatie en een lijst met gebruikte afkortingen.

2. Stand van zaken privacy binnen de gemeentelijke organisatie

Allereerst volgt een globaal overzicht van de 'stand van privacy' bij de gemeente Nijmegen (§2.1).
Dit geschiedt op basis van een 'Quick Scan privacy' waar langs het kwadrant van de SWOT-analyse (Sterkte, Zwakte, Kansen, en Bedreigingen) in één oogopslag de huidige stand van zaken wordt weergeven.

Het control systeem 'Cybermanager' is inmiddels zo goed als ingericht. Dit is geschied op basis van het VNG/ IBD-borgingsproduct 3.0. Dit is een landelijk vastgestelde normering op het gebied van (naleving van) privacy.
Voor de derde keer is er een 'interne audit' uitgevoerd op de privacy maatregelen die opgenomen zijn in de Cybermanager. Deze audit is in het vierde kwartaal van 2024 uitgevoerd met hulp van de privacy ambassadeurs die binnen de afdelingen werkzaam zijn en aangevuld door het team privacy en het team informatiebeveiliging. Het geeft inzicht in de aspecten die nog verbetering behoeven binnen de organisatie (§2.2).

Tenslotte (§2.3) volgt een korte passage over de voortgang van de maatregelen uit het Rekenkameronderzoek (2022) naar de huidige stand van Informatiebeveiliging en Privacy binnen de gemeentelijke organisatie. Voor de inhoud hiervan verwijs ik naar de rapportage zelf.

2.1 Quick scan Privacy

De quick scan wordt weergegeven langs de vier kwadranten van 'sterk', 'zwak', 'kans' en 'bedreiging'.
Als inkleuring van die begrippen de volgende leidraad:

- Sterk: beschrijving van wat je ziet, ervaart, hoort wat als sterk / positief beschouwd kan worden. *Voor sturing vanuit het management betekent dit: draag zorg voor behoud van deze waarden.*
- Zwak: idem maar dan zwak / negatief. *Voor sturing vanuit het management betekent dit: zorg ervoor dat deze acties en handelingen stoppen.*
- Kans: beschrijving van een beweging, richting, koers of trend die als positief of kansrijk ervaren kan worden. Dat hoeft dus niet feitelijk zo te zijn. Het gaat er hier om dat je dit soort bewegingen, signalen of "kansen" ziet en wilt duiden. *Voor sturing vanuit het management betekent dit: zet méér energie (inzet mensen en het geven van prioriteit) op deze kansen.*
- Bedreiging: idem maar dan als negatief en bedreigend. *Voor sturing vanuit het management betekent dit: bespreek regelmatig deze bedreigingen en onderneem acties daartegen.*

SWOT Privacy

Om een snel inzicht te krijgen in de problematiek volgt hieronder een SWOT-analyse gebaseerd op aspecten, producten en gremia binnen de wereld van privacy bij de organisatie gemeente Nijmegen.

NB. Gebruikte afkortingen worden verklaard in bijlage 2.

SWOT Privacy 2024

Sterk

- Privacy afspraken: opzet en bestaan
- Privacybeleid (is vastgesteld door de Raad in 2023)
- Leerlijnen via Studytube
- Intake procedure: deze geeft een vangnet en is effectief
- Afhandeling van klachten en incidenten
- Afhandeling en registratie Datalekmeldingen
- DPIA als instrument: dit wordt steeds meer gemeen goed. Aantal is hoog gebleven. Is positieve indicatie van bewustzijn.
- Verwerkersovereenkomsten als instrument
- Privacy Protocollen als instrument
- Audit Wpg en vervolgafspraken: voor de komende twee jaar is er een vervolg ingezet. Ziet er veel belovend uit.
- De kwaliteit van de beschrijving van de naleving is enorm verbeterd. Meerdere afdelingen geven uitgebreid en inhoudelijk toelichting hierover.
- Privacybeleid is voorzien van KPI's voor meting
- Specifieke aandacht voor privacy in de afdeling.
  'Good practise': VSA team privacy en informatiebeveiliging.
- 'Best Practise': Opzet, bestaan en werking 'Mijn afdeling AVG proof' door de afdeling Stadsrealisatie.

Zwak

- Privacy afspraken: werking. Hieraan wordt gewerkt maar is niet (volledig) op orde.
- Bewustzijn is nog niet verankerd in de organisatie
- Kennis en Kunde. Deze is nog niet goed geland in de organisatie
- Naleving: deze is nog net op orde. De wil is er wel, maar niet elke afdeling lukt het hier mee om te gaan.
- Naleving verwerkersovereenkomsten: 1. Zeer matige score (30%) op de naleving van de contracten; 2. Vaak is het tekenen van het contract het einde van het contact met de leverancier.
- Risicomanagement: wel in beeld als belangrijk aspect. Niet geoperationaliseerd.
- Samenwerkingsverbanden en regietafels: volledig overzicht ontbreekt.
- Informeren betrokkenen en een onderliggend communicatieplan ontbreken nog (zie uitkomsten zelfevaluatie). We kunnen de informatie naar betrokkenen veel beter vormgeven. Hiertoe moet een traject opgestart worden.
- Melding datalekken: het is onduidelijk of deze allemaal gemeld worden.

Kans

- Bewustzijnscampagnes werken; inmiddels budget verkregen
- Acceptatie: deze groeit door kennis en kunde
- Risk Appetite: wordt vaak genoemd maar is nog niet geoperationaliseerd. Gaat ons helpen.
- Idem: evidenced based accountability. 'Best practices' vanuit de organisatie van de afdeling IZL.
- Tafel van 11 als methodiek voor naleving. Kennis en kunde hiervan gaat de organisatie helpen om 'spontane naleving' als strategie in te zetten.
- Derde Interne Privacy Audit via Cybermanager: helpt ons in het focussen op de risico's die ertoe doen.
- Privacy ambassadeurs: grote groep enthousiaste medewerkers verdeeld over de teams binnen de afdelingen.
- Privacy ambassadeurs zijn wederom betrokken bij de interne audit
- *Externe* ethische Digitale Commissie: adviezen zijn waardevol voor de organisatie.
- Mogelijke inrichting *interne* ethische commissie.
- Verbeteraanpak CORSA: stap voor stap verbetering. Nieuwe DPIA vrijwel gereed (afronding 2025).

Bedreiging

- Omvang van het team privacy: met de kennis en kunde zit het wel goed. Alleen de omvang van de formatie schiet te kort. Hierdoor ontstaan achterstanden in verwerking van DPIA's, adviezen met betrekking tot en zicht op verwerkersovereenkomsten en privacy protocollen en het bijhouden van nieuwe ontwikkelingen.
- Implementatie in het Sociale Domein: er zijn in 2025 wel extra middelen beschikbaar, vraag is of dit voldoende is om achterstand weg te werken.
- Acceptatie van verplichte leerlijnen: blijf zorgen voor duidelijke communicatie over nut en noodzaak, tevens voor budget
- Werking van (= het nakomen van en verantwoording over) de maatregelen opgenomen in de projectplannen van 'Mijn afdeling AVG Proof'. Deze is nog niet goed ingericht.
- Blijvende naleving van de DPIA's. Wordt vergroot door 100% toetsing op naleving. Moet niet een eenmalige actie worden,
- Ontbrekend (totaal) overzicht over de verwerkingsovereenkomsten.
- Audits op privacy protocollen: zicht hierop ontbreekt nog. In 2025 meer focus op samenwerkingsverbanden.
- Externe factoren zoals cybercriminaliteit, datalekken, technische storingen of andere onvolmaaktheden.

2.2 VNG AVG Borgingsproduct 3.0 jaar 2024

In onderstaande tabel geven we de resultaten weer van de interne audit op basis van de 'VNG AVG Borging 3.0' voor het jaar 2024.
Tot en met 2023 werkten we met 'het borgingsproduct 2.0' van de VNG/IBD als instrument om naleving van de AVG te meten.
Vanaf 2024 is het 'borgingsproduct 3.0' geïntroduceerd. Deze is op onderdelen uitgebreider dan zijn voorganger.
Hieronder geven wij de scores weer op het niveau van hoofdindeling en eerste laag van verbijzondering. In het systeem Cybermanager kunnen we nóg verder inzoomen in een tweede (gedetailleerdere) laag. Voor de overzichtelijkheid houden we het hier op 2 niveaus.

No.	Hoofdindeling	Product of proces	Score opzet %	Score Bestaan %	Score werking %
1.	Beleid		🟢	🟢	🟠
1.1		Beleid vaststellen	100	100	75
1.2.		Privacy beleid	100	100	75
1.3.		Verantwoordelijkheden	100	100	88
2.	Processen		🟢	🟢	🟠
2.1.		Processen	100	100	50
2.2.		Verwerkingsregister	100	100	33
2.3.		Pré DPIA	100	100	88
2.4.		DPIA	100	100	81
2.5.		Bewaar- en vernietigingstermijnen	100	100	75
3.	Organisatorische inbedding		🟢	🟠	🔴
3.1.		Privacy team	100	67	33
3.2.		Aanstelling FG	100	75	75
3.3.		Informeren OR	100	100	25
3.4.		Bewustwording	100	100	38
4.	Rechten van betrokkenen		🟠	🟠	🔴
4.1.		Recht op informatie	50	50	12
4.2.		Processen rechten van betrokkene	100	100	50
4.3.		Toestemming	100	100	50
4.4.		Geautomatiseerde individuele besluitvorming	50	50	0
4.5.		Websites en applicaties	100	100	50
4.6.		Technische ondersteuning	100	100	69
5.	Samenwerking		🟢	🟢	🟠
5.1		AVG rollen	100	100	69
5.2		Gegevensverstrekking	100	100	69
6.	Gegevensbescherming		🟢	🟢	🔴
6.1		Risico's	100	100	0
6.2		Gegevensbescherming door ontwerp	100	100	25
6.3		Gegevensbescherming door standaardinstellingen	100	100	50
6.4		Informatiebeveiliging	100	100	50
6.5		Privacy incidenten en datalekken	100	100	81
7.	Verantwoording		🟢	🟢	🟠
7.1.		Evaluatie naleving AVG	100	100	67
7.2		Evaluatie informatiebeveiliging	100	100	62
7.3		Rapportage	100	100	75

In bijlage 1 wordt gedetailleerder ingegaan op de scores van de interne audit die jaarlijks met de privacy ambassadeurs is gedaan.
Voor meer informatie: https://www.informatiebeveiligingsdienst.nl/product/avg-borgingsproduct-3-0-documentatie

Conclusies interne audit op basis van borgingsproduct 3.0 van de VNG/IBD

Zoals de tabel laat zien zijn over het algemeen de verschillende aspecten van Privacy goed beschreven (opzet) en ingeregeld (bestaan). De uitvoering hiervan (werking) laat (helaas) te wensen over (gele en rode scores).
Specifiek op de onderwerpen 'Rechten van betrokkenen', 'Organisatorische inbedding' en 'Gegevensbescherming' moet nog veel effort verricht worden om de 'werking' op orde te krijgen. Hier scoort de organisatie een duidelijke 'onvoldoende' (score 'rood' bij werking). Voor meer informatie: zie bijlage 1.

2.3 Rapportage rekenkameronderzoek informatiebeveiliging en privacy

In 2022 heeft de Rekenkamer van de gemeente Nijmegen haar rapportage inzake Informatiebeveiliging en Privacy aan de gemeenteraad aangeboden. Voor de volledige inhoud klik hier. In het Rekenkameronderzoek stellen de onderzoekers (pp 14-15): *"voor Nijmegen schatten de onderzoekers het volwassenheidsniveau voor privacybescherming hoger: tussen de 2 en 3."*

In de reactie op het onderzoek geeft het college aan te streven naar volwassenheidsniveau 3 (op het gebied van privacy) als realistisch doel voor de komende jaren (zie uitleg hiervan: bijlage 3).
Als FG van de gemeente Nijmegen ondersteun ik dit streven.
In onderstaande tabel omschrijven we kort de aanbevelingen die de Rekenkamer gedaan heeft. Tevens de beschrijving van de voorgestelde acties (die er mede toe moeten leiden te komen tot het volwassenheidsniveau 3, binnen vier jaar), inclusief een inschatting van de planning (op kwartalen gebaseerd) voor het aspect privacy.

	Omschrijving aanbeveling rekenkameronderzoek be4treffende privacy	Voorgestelde actie	Planning
1.	Verhelder Beleid informatiebeveiliging en privacybescherming	Privacy beleid door College en de Raad vastgesteld medio 2023.	Voor privacy Afgerond
2.	Aanvulling ontbrekende onderdelen beleid	Middels strategisch privacy beleid	Afgerond
3.	Organisatie brede risicoscan	Uitgevoerd door externe organisatie (2023)	Afgerond
4.	Risicomanagement tot continue proces	Eerste inventarisatie en opzet voor vervolg	Geen vervolg gegeven
5.	Stel voldoende middelen beschikbaar	Er zijn extra middelen beschikbaar of dat voldoende is, moet nog blijken	Besluit in 2023; uitvoering 2024/5
6.	Geef CISO en FG eigen budget	Niet specifiek bij deze functies belegd; wel bij Stadscontrol	Afgerond
7.	Afspraak over toetsing en rapportage	ENSIA op gebied van beveiliging Interne audit Privacy	Q4 2024
8.	Gebruik KPI's	Door de Raad vastgesteld en opgenomen in de rapportages aan de Raad	2024 vastgesteld
9.	i-bewustzijn	Doorlopende campagne. Mede onderdeel van de opgave 'digitale transformatie'	Continue
10.	Vaststellen informatiebeveiliging en privacy beleid in de Raad	Update strategisch privacy beleid	Eind Q2 2023 vastgesteld
11.	Informeren van Raad door bv CISO en FG of externe deskundigen	Middels Raadsbrief; Jaarverslag FG wordt aan College en Raad aangeboden	Afgerond; speelt elk jaar
12.	Vastleggen controlerende rol	Onderdeel van strategisch privacy beleid	Afgerond
13.	Accountant IT audit	Via Stadscontroller, CISO en CIO	doorlopend

3. Uitvoering Privacy beleid

3.1 Privacy beleid update

In juli 2023 is het nieuwe privacy beleid door de Raad vastgesteld. Het oude beleid stamde uit 2018 en was toe aan vervanging, gelet op het feit hoe het belang van het thema 'privacy' binnen de gemeente sinds 2018 gegroeid is. Het nieuwe beleid schetst de visie op het respecteren van de persoonlijke levenssfeer van onze inwoners, de gewenste transparantie naar de inwoner, het belang van het beschermen van persoonsgegevens en de afweging die gemaakt dient te worden tussen dienstverlening enerzijds en het beschermen van persoonsgegevens anderzijds. Daarnaast wordt de ethische kant van privacy belicht. Verder is hiermee de ambitie uitgesproken om binnen vier jaar (2027) het volwassenheidsniveau 3 te bereiken.

3.2 Rechten van betrokkenen

In 2024 zijn er bij de gemeente 29 inzageverzoeken ingediend. Geen verwijderverzoeken. Dit is een flinke daling ten opzichte van 2023, die te verklaren is doordat er een nieuw formulier op de website is toegevoegd om BRP-inzageverzoeken in te dienen. Daardoor zijn deze verzoeken niet meer bij team privacy terechtgekomen. Verder zijn er twee bezwaren aangetekend tegen de besluiten op inzageverzoeken. Deze zijn afgehandeld.

3.3. Incidenten en Datalekmeldingen

In 2024 zijn er 96 beveiligingsincidenten gemeld. Daarvan waren 81 meldingen intern en 15 meldingen extern, waarvan 1 responsible disclosure melding (digitale klokkenluidersregeling).
Er waren 10 datalekken. Van de datalekken zijn er 9 bij de Autoriteit Persoonsgegevens (AP) gemeld.
Eén is niet gemeld, omdat het hier ging om alleen geboortedata van 19 ontvangers van de lintjes, waarbij de gegevens al openbaar waren.
Als het gaat om beveiligingsincidenten dan gaat de verkeerd verstuurde mail nog steeds aan kop.
De inrichting van de CyberManager komt steeds meer op orde. Hierdoor kunnen we over de meldingen steeds meer informatie verstrekken. De 96 van het afgelopen jaar kunnen we bijvoorbeeld categoriseren naar oorzaak:

Privacy of beveiligingsincident:	46
Verlies / diefstal:	13
Social engineering:	12
Schending privacy wetgeving:	1
Kwetsbaarheid:	23
Schending fysieke beveiliging	1

3.4. Afhandeling Klachten

In 2024 zijn er in totaal 8 klachten ingediend door burgers en medewerkers betreffende een onrechtmatige verwerking van hun persoonsgegevens. Alle klachten zijn behandeld en naar behoren afgerond.

3.5. Onderzoek door of namens de FG, postbus FG

Daarnaast hebben meerdere burgers zich rechtstreeks tot de FG gericht middels de functionele e-mailbox Functionarisgegevensbescherming@nijmegen.nl. Dit betrof veelal vragen om nadere informatie en uitleg over proces en procedures. In 2024 zijn er op deze wijze 7 verschillende klachten, verzoeken of andersoortige vragen rechtstreeks aan de FG van de gemeente Nijmegen gestuurd. Alle klachten, vragen en informatieverzoeken zijn door de organisatie van de gemeente Nijmegen naar behoren afgehandeld.

4. Check op de naleving op basis van interne controle 2024.

4.1. Uitvoering van de plannen van aanpak 'Mijn afdeling privacy proof'

Medio 2022 zijn de afdelingen begonnen om de uitvoering van het traject "Mijn afdeling AVG-proof" weer op te pakken, na stilstand door de Coronapandemie. Alle afdelingen hebben dit traject inmiddels afgerond. Afronding van het traject - Mijn afdeling AVG-proof - betekent nog niet dat de afdelingen ook daadwerkelijk AVG-proof zijn. De eerste stap hiertoe is dan gemaakt. In de trits 'opzet – bestaan – werking' is de eerste fase dan afgerond: 'de opzet'. De processen zijn in beeld, er is duidelijk wat er (nog) moet gebeuren en de acties zijn ingepland. In dit nalevingsonderzoek is die planning gevolgd (de handelingen rondom het 'bestaan': het vaststellen dat maatregelen werken zoals beschreven) en zijn de acties beoordeeld (volgen van de 'werking' en naleving van de opzet en verantwoording hierover).
In de tabel per afdeling zijn de scores op de naleving vermeld naar aanleiding van de uitkomsten van het controlplan 2024 door de FG.

Stand per eind 2023

Afdeling	Opzet	Bestaan	Werking
Financiën (FA)	🟢	🟠	🟠
Inkomen, Zorg en Leerrecht (IZL)	🟠	🟠	🟠
Maatschappelijke Ontwikkeling (MO)	🟢	🟠	🔴
Personeel, Informatie en Facilitair (PIF)	🟢	🟠	🟠
Publiekszaken (PU)	🟢	🟢	🟠
Stadsbeheer (SB)	🟢	🟠	🟠
Stadsontwikkeling (ST)	🟢	🟠	🟠
Stadsrealisatie (SR)	🟢	🟢	🟠
Vastgoed, Sport en Accommodaties (VSA)	🟢	🟢	🟠
Veiligheid, Juridische Zaken en Bestuursondersteuning (VJB)	🟢	🟢	🟠

Stand per eind 2024

Afdeling	Opzet	Bestaan	Werking
Financiën (FA)	🟢	🟢	🟠
Inkomen, Zorg en Leerrecht (IZL)	🟢	🟠	🟠
Maatschappelijke Ontwikkeling (MO)	🟢	🟠	🟠
Personeel, Informatie en Facilitair (PIF)	🟢	🟠	🟠
Publiekszaken (PU)	🟢	🟢	🟠
Stadsbeheer (SB)	🟢	🟠	🟠
Stadsontwikkeling (ST)	🟢	🟠	🟠
Stadsrealisatie (SR)	🟢	🟢	🟢
Vastgoed, Sport en Accommodaties (VSA)	🟢	🟢	🟠
Veiligheid, Juridische Zaken en Bestuursondersteuning (VJB)	🟢	🟢	🟠

Nadere informatie is beschikbaar bij de FG en het management van elke afdeling. Dit betreft de uitkomsten van de 'Uitvoering Controlplan FG Bevindingen Naleving 2024' per afdeling, zoals vastgesteld door de Directie in mei 2025.

4.2. Wpg Audit

In 2022 heeft de (verplichte) externe audit op naleving van de Wet Politiegegevens (Wpg) plaatsgevonden. Voorjaar 2023 is hierop een (externe) hercontrole uitgevoerd en najaar 2023 een eerste interne controle. De resultaten van de externe controles zijn verstuurd aan de Autoriteit Persoonsgegevens. In een reactie op de audit 2022 heeft de organisatie het volgende in de rapportage aan de Autoriteit laten opnemen (par. 3.2.):

> Wij herkennen ons in het 'oordeel met beperkingen', zoals weergegeven in tabel 1.12 voor de drie onderzochte domeinen.
> Streven voor jaarschijf 2022:
> Het kalenderjaar-2022- willen we gebruiken om de 'opzet' op alle onderdelen aan de norm te laten voldoen (mits dat ook met partners zoals leveranciers geregeld kan worden). In termen van de gehanteerde kleurscore: groen (voldoet aan de norm) of minimaal geel (voldoet deels aan de norm).
> Daarnaast willen we het 'bestaan' (streven score 'groen' of in uiterste gevallen minimaal 'geel') en de 'werking' (minimaal 'geel') verbeteren. Uiteindelijk is ons streven om in 2023 zoveel mogelijk 'aan de norm te voldoen' (kleurcode groen), voor zover dat mogelijk is vanuit afhankelijkheid van derde partijen.
>
> De externe auditeur '2-Control B.V.' stelt in haar rapportage:
> "Wij hebben vastgesteld dat Gemeente Nijmegen niet (geheel) voldoet aan het bij of krachtens de wet bepaalde. Inzake de uitvoering van de hercontroles, bevelen wij Gemeente Nijmegen aan om deze door een externe auditor te laten uitvoeren. Wij baseren deze aanbeveling op het feit dat de Gemeente Nijmegen op dit moment nog geen interne auditor heeft en heeft daarmee niet de mogelijkheid om de hercontrole zelf uit te voeren."
> Wij zijn voornemens deze aanbeveling over te nemen voor het kalenderjaar 2022. Voor de toekomst (2023 en verder) willen wij met interne auditors gaan werken.
> In het najaar 2022 willen we de interne audit weer opstarten. Tot die tijd zal actief gestuurd worden op het realiseren van de aanbevelingen met als doel bovengenoemd streven voor 2022 te realiseren.

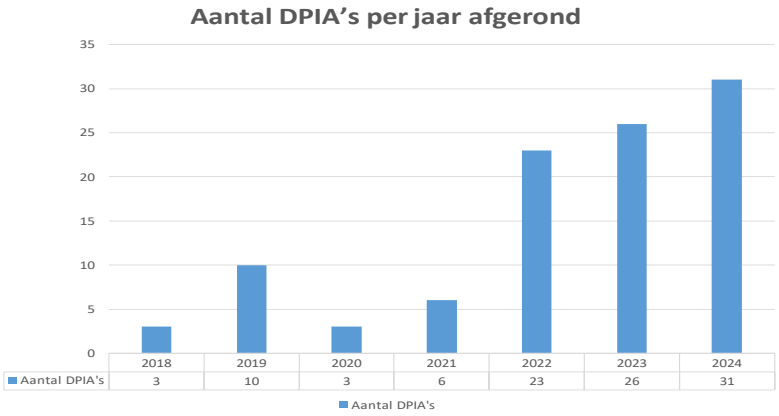
Inmiddels is er een traject gestart om de noodzakelijke verbeteringen in dit traject op te pakken en vorm te geven. In het najaar 2022 is er reeds een interne (tweede) audit geweest op dit domein door een interne auditeur, die hiervoor in de organisatie benoemd is. Hier werden reeds de eerste vorderingen opgemerkt.
In het voorjaar 2023 is de verplichte (externe) hercontrole op de eerste audit Wpg uitgevoerd. Ook deze is verzonden aan de AP. De resultaten waren op het eerste oog teleurstellend. In het sociale domein waren wel stappen gezet, in het fysieke domein was sprake van achteruitgang. Inzoomend is dat te verklaren: de opzet was in eerste instantie nog als redelijk bestempeld, en nu als onvoldoende. Oorzaak was dat ten tijde van de hercontrole de gehele opzet vernieuwd werd en dat proces was nog gaande.
Bij de interne controle die in het najaar 2023 op het fysieke domein is gehouden, bleek dat dit inmiddels weer hersteld is. De nieuwe opzet is beter dan de oude en ook in het fysieke domein is sprake van een goede vooruitgang ten opzichte van de eerste externe audit.

In 2024 is er conform planning een interne audit gehouden op het gebied van Leerrecht. Belangrijkste bevindingen zijn dat er een betere autorisatie controle is ingevoerd en verbeteringen zijn aangebracht in de processen ten behoeve van archivering. Ook is het handboek is verder geoptimaliseerd. Zo is er meer beschreven over de wettelijke verplichting en taken/vuistregels rondom verwerking van (politie)gegevens. Het advies is om met de leverancier contact op te nemen, om de logging te verbeteren.

Overige bijzonderheden uit deze interne audit van 2024: doordat DPIA's voor de onderwerpen in scope nog niet volledig afgerond zijn of actueel zijn, ontbreken handvatten voor de toezicht maatregelen. Hierdoor bestaat het risico dat de toezicht maatregelen onvoldoende invulling hebben gekregen. Het proces voor het actueel houden van verwerkingsregisters lijkt niet geformaliseerd. Wij adviseren hier een proces voor in te richten.
Tenslotte is aangeraden om logging van systemen te optimaliseren.

4.3. DPIA als continu bijstuurproces

Het instrument DPIA is nog steeds te veel een momentopname van de privacy risico's die spelen bij een gegevensverwerking. Ook wordt het instrument nog niet voldoende ingezet als monitoring op de implementatie en de borging van de ingezette maatregelen op de langere termijn. Hier schuilt dan ook nog steeds een kwetsbaarheid in. Door de ombuiging van implementatie naar beheer / controle is de DPIA inmiddels een blijvend onderdeel van de (interne) verantwoordingsplicht. In 2024 zijn in totaal 31 DPIA's uitgevoerd op grote complexe gegevensverwerkingen binnen het fysiek, sociaal en veiligheidsdomein. In de jaarlijkse controle wordt getoetst in hoeverre uitvoering en borging wordt gegeven aan de mitigatie (verzachting/vermindering) van risico en maatregelen zoals opgenomen in de DPIA's.



In het totaal zijn er tot en met 2024 102 DPIA's afgerond (zie bovenstaande grafiek).
Voor de uitvraag naar naleving is de (verval)datum van 1 oktober 2024 gehanteerd. Op dat moment waren 93 DPIA's afgerond. Een aantal DPIA's zijn niet meer valide omdat het project is afgerond, opgehouden is te bestaan of de verouderde DPIA vervangen is door een nieuwere. Hieronder in een schema de naleving per afdeling van de 80 DPIA's die op vervaldatum 1 oktober 2024 nog actueel waren.

Afdeling	Totaal	Naleving op orde	Naleving Deels op orde	Naleving niet op orde
Oordeel =>		🟢	🟠	🔴
Financiën (FA)	5	5		
Inkomen, Zorg en Leerecht (IZL)	19	17	2	
Maatschappelijke ontwikkeling (MO)	12	6	6	
Personeel, Informatie & Facilitair (PIF)	10	4	5	1
Publiekszaken (PU)	8	8		
Stadsbeheer (SB)	9	8	1	
Stadsontwikkeling (ST)	1	1		
Stadsrealisatie (SR)	2	2		
Veiligheid, Juridische Zaken, Bestuursondersteuning en Advies (VJB)	13	13		
Vastgoed, Sport en Accommodaties (VSA)	1	1		
Totaal	*80*	*65*	*14*	*1*

4.4. Register van Verwerkingen

De AVG stelt het verplicht voor organisaties om in een register bij te houden welke persoonsgegevens worden verwerkt, met welk doel en met welke middelen. Het Register van Verwerkingen van de gemeente Nijmegen wordt in het kader van het manifest 'Open en Weerbaar' gepubliceerd op de website. Het publiceren van het register van verwerkingen is overigens geen wettelijke verplichting.
Als FG wil ik dat álle verwerkingen met mogelijk hoog risico waarin met persoonsgegevens wordt gewerkt, in de komende jaren van een DPIA worden voorzien. Hierbij wordt het Register van Verwerkingen als basis gehanteerd. Voor de organisatie van de gemeente Nijmegen is dit nog een grote opgave is (en tevens een inhaalslag).

Onderstaand een overzicht per afdeling, waarin duidelijk wordt op welke wijze de afdeling 'in control' is wat betreft naleving van de verwerkersovereenkomsten gerelateerd aan een *vastgestelde* DPIA. De organisatie heeft daarnaast nog meerdere verwerkersovereenkomsten afgesloten die níet gerelateerd zijn aan een DPIA. Die zijn in dit overzicht níet meegenomen. Er is wel navraag gedaan naar naleving. Deze is bedroevend (Controlplan 2024).

Niet elke vastgestelde DPIA kent één verwerkersovereenkomst, sommige hebben meerdere verwerkers, een groot aantal kent géén 'externe' verwerker. Daarvan is meestal de IRvN de verwerker. Met de IRvN is één verwerkersovereenkomst afgesloten voor alle applicaties die zij onder beheer hebben. Naleving vindt plaats via de afdeling PIF. Dat betekent dat voor een groot aantal DPIA's deze niet nogmaals beschreven hoeft te worden.
Het aantal verschillende overeenkomsten bij DPIA's (49) komt daarmee niet overeen met het aantal vastgestelde DPIA's (93).

Afdeling	Totaal	Naleving op orde	Naleving Deels op orde	Naleving niet op orde
Oordeel =>		🟢	🟠	🔴
Financiën (FA)	5	5		
Inkomen, Zorg en Leerecht (IZL)	7	1		6
Maatschappelijke ontwikkeling (MO)	10	2	1	7
Personeel, Informatie & Facilitair (PIF)	7	3		4
Publiekszaken (PU)	5	2		3
Stadsbeheer (SB)	8			8
Stadsontwikkeling (ST)	1	1		
Stadsrealisatie (SR)	2	2		
Veiligheid, Juridische Zaken, Bestuursondersteuning en Advies (VJB)	3		2	1
Vastgoed, Sport en Accommodaties (VSA)	1		1	
Totaal	*49*	*16*	*4*	*29*

Oordeel over de naleving van de afspraken uit verwerkersovereenkomsten

De resultaten uit deze steekproef zijn nog niet hoopgevend. Slechts 33% van de respondenten geeft aan een verwerkersovereenkomst na te leven. 8 % doet dat deels. En van de anderen 59% is óf geen inzicht verkregen óf wordt er níet nageleefd. De organisatie is wat betreft AVG nog níet taakvolwassen genoeg om dit adequaat op te pakken. Na vier jaar uitvraag is dit wel teleurstellend te noemen.
Hiermee is op dit aspect 'volwassenheidsniveau 3' nog ver uit het zicht.

4.5. Tafel van Elf

De resultaten uit het controlplan 2024 worden weergegeven in onderstaande tabel. Daarbij maak ik gebruik van de ‘Tafel van Elf’, ontwikkeld door het ministerie van Justitie. Deze methodiek ondersteunt de analyse van nalevingsgedrag. In het domein van privacybescherming is ‘naleving’ één van de cruciale aspecten in houding en gedrag. Naleefgedrag komt immers niet uit de lucht vallen. De mate van naleefgedrag van vastgestelde regels en uitgangspunten wordt door een aantal aspecten beïnvloed. Deze aspecten vormen samen de ‘Tafel van Elf’.

Aspecten Tafel van 11	Dimensie	Bekendheid	Duidelijkheid	Aandachtspunten / vervolgacties
Spontane Naleving				
	Kennis van regels	Laag tot middel	Laag tot middel	Na opgedane kennis is de acceptatie hoger. Dit is met name merkbaar bij de privacy ambassadeurs. Doel en werking DPIA’s is bekender geworden. Doel en werking verwerkersovereenkomsten is nog steeds te laag. ‘Leren en Ontwikkelen’ is verbeterd door verplicht inzet leerlijnen. Privacy Ambassadeurs worden steeds meer ingezet en hebben dit jaar (wederom) meegedaan aan de privacy scan. Actie: blijvend verhogen kennis en kunde binnen de organisatie.
	Kosten / Baten	Middel	Middel	Na kennis: acceptatie hoog. Mogelijke kans op boetes (voorbeelden komen van andere instanties) zorgt voor meer gevoel van urgentie.
	Mate van Acceptatie	Middel tot hoog	Middel	Na kennis: acceptatie hoog. Privacy ambassadeurs meer bekend maken ín de afdelingen. Nóg meer gebruik van maken.
	Normgetrouwheid doelgroep	Middel tot hoog	Middel	Hier spelen de privacy ambassadeurs een rol. Die rol kan verder uitgewerkt worden
	Niet overheidscontrole: Sociale controle / horizontaal toezicht	Middel	Middel	Niet ingezet Sociale controle: afwegen. Impliciet via de privacy ambassadeurs. Horizontaal toezicht: inbedden.
Handhaving				
	Meldingskans	Laag	Laag	Kan voorkomen via externe melding (burger, instantie of AP); (nog) niet expliciet voorgekomen.
	Controlekans	Laag	Middel, wordt hoger	Deze is verhoogd en geeft effect. Aanlevering is zowel in tijd als kwaliteit beter dan in 2023. Control uitvraag wordt de meeste afdelingen ingepland in P&C cyclus.
	Detectiekans	Laag	Laag tot middel	Verwerkersovereenkomsten derde steekproef; In 2024 is deze uitgebreid naar álle overeenkomsten. In eerste instantie gericht op verwerkersovereenkomsten gerelateerd aan een DPIA. DPIA’s worden allen op naleving getoetst. De detectiekans is dan 100%.
	Selectiviteit	Laag	Laag	Onderscheid middels stoplichten de mate van naleving. Dit heeft effect. Rood stoplicht zorgt voor urgentie.
	Sanctiekans	Laag	Laag	(Nog) Niet geoperationaliseerd.
	Sanctie ernst	Laag	Laag	(Nog) Niet geoperationaliseerd.

4.6. Privacy Protocollen

In een privacy protocol ligt vast met welk doel persoonsgegevens worden verwerkt, wie voor welke acties met betrekking tot persoonsgegevens verantwoordelijk is, wanneer er sprake is van gezamenlijke verantwoordelijkheid en hoe invulling wordt gegeven aan de vereisten uit privacy wet- en regelgeving zoals: de informatieplicht, de rechten van de betrokkene, beveiliging en het bewaren en vernietigen van persoonsgegevens. Afdelingen hebben inmiddels een beter beeld van de diverse privacy protocollen die afgesloten zijn.
Twijfels blijven bestaan of álle privacy protocollen met deze uitvraag in beeld zijn. Positief is dat er méér in beeld zijn én de eerste nalevingsrapportages ontvangen zijn. Met name de afdeling VJB/Veiligheid kent meerdere protocollen. Financiën (FA), Stadsbeheer (SB), Stadsrealisatie (SR, Stadsontwikkeling (ST), en Vastgoed, Sport en Accommodaties (VSA) kennen – voor zover bekend – geen privacy protocollen.

Naleving privacy protocollen (voor zover bekend)

Naam Privacy Protocol	Afdeling	Naleving
Protocol Gebruik anonieme accounts bij onlineonderzoek	IZL	🟢
Overeenkomst uitwisseling persoonsgegeven thuiszitters SWV - gem Nijmegen (Leerrecht)	IZL	🟢
Diverse Overlegtafels (De meesten zijn nog niet in beeld)	MO	🔴
Privacy protocol Leer Platform Study Tube.	PIF	🟢
Protocol Gebruik anonieme accounts bij onlineonderzoek	PU	🟢
Meldpunt Ondermijning	VJB	🟢
IGP (Intelligence Gestuurd Werken)	VJB	Wordt uit gefaseerd
Protocol Gebruik anonieme accounts bij onlineonderzoek	VJB	🟢
RIEC's-LIEC	VJB	Onzeker
Regieteams	VJB	🟢
Zorg- en Veiligheidshuis	VJB	🟢
Nederlandse Code voor Onderzoek en Statistiek/Handboek AVG en statistisch onderzoek	VJB	🟢
Communicatie: Instructie inzake verwerken persoonsgegevens bij aanvragen Koninklijke Onderscheidingen.	VJB	🟢

4.7. Archivering / vernietiging

Ook in 2024 heeft het project Corsa AVG-proof aandacht van de FG gehad. Corsa is het algehele zaaksysteem waarin alle relevante dossiers in verwerkt, opgeslagen en bewaard worden. Waar nodig en noodzakelijk wordt overgegaan tot vernietiging. Probleem met Corsa was dat in principe iedereen die geautoriseerd was en hiermee toegang tot het systeem kreeg, ook alles kon zien. Besloten is bij iedereen de autorisatie weg te halen, die toegang geeft tot alle documenten en meta-data (uitzetten functie: 'OallenLezen').
Vervolgens zijn de medewerkers alleen nog geautoriseerd voor dat deel van de taken die noodzakelijk zijn en passend zijn bij de uitvoering van hun werk. Per onderdeel is bepaald welke zaaktype/werkproces er wordt uitgevoerd, welk bureau hieraan gekoppeld is en welke functies de dossiers/documenten mogen inzien dan/wel wijzigen. Belangrijk te benoemen is dat Corsa met bovenstaande werkwijze nog steeds niet AVG-proof is! Daarvoor moeten nog méér stappen ondernomen worden. Maar het risico op privacy schendingen zijn door deze twee ingrepen wel drastisch verminderd.

5. Bewustwording en weerbaarheid

5.1. Vergroting I-bewustzijn

Om meer gestructureerd aandacht te besteden aan iBewustzijn is verplichte scholing onderdeel van de jaarlijkse plannen. Om de effectiviteit van deze interventies beter te kunnen bepalen is de Hogeschool Saxion gevraagd om een onderzoek naar het iBewustzijn binnen de gemeente en het ontwikkelen van een instrument om deze op een efficiënte manier inzichtelijk te maken. De interventies met Saxion vinden in 2025 plaats.

In 2024 zijn de volgende iBewustacties uitgevoerd:

In het eerste kwartaal bezocht de operational security officer diverse teams met uitleg over hoe en wanneer veilig te mailen (Zivver). Tegelijkertijd werd het gebruik van wachtwoordmanager Bitwarden aanbevolen. De IRvN stelt deze beschikbaar om wachtwoorden veilig op te kunnen slaan.
Een steekproef met een ‘mystery guest’ ter bepaling van een ‘clear screen & clean desk’, resulteerde in 2024 in een score van 80% (ten opzichte een gedragsmeting van 40% uit het rapport ‘Cyberchallenge Troje’).
In de maand maart ontvingen medewerkers een mail via Studytube om de ‘herhalingstraining informatiebewustzijn’ te voltooien. Ten opzichte van 2023 (70%) is de score gedaald naar 60%.
Tijdens het Let’s Connect festival, hebben meer dan 70 medewerkers deelgenomen aan ‘Nimma Hackt’.
Van 1 oktober tot en met 31 december heeft een phishing campagne plaatsgevonden bij 4 teams: Financiën, P&O, Publiekszaken en JZ. De resultaten zijn met hen besproken.
In november vond het NYMACON hack evenement plaats bij Waalhalla in Nijmegen in samenwerking met IRvN, cyber security dienstverlener Hunt & Hackett, het Institute for Computing and Information Sciences van de Radboud Universiteit Nijmegen. De evaluatie met de studenten en IRvN was positief. Het evenement krijgt een vervolg in 2025.

5.2. Privacy Ambassadeurs

In 2024 zijn er 2 bijeenkomsten geweest met de groep privacy ambassadeurs. Deze groep is iets gegroeid.
Op dit moment heeft bijna elk team / bureau een ambassadeur. In het totaal kent de gemeentelijke organisatie op dit moment 49 privacy ambassadeurs (44 in 2023).
Afspraak is dat elk bureau in een afdeling minimaal één ambassadeur dient te hebben.

Dit betekent dat hiermee een directere verbinding met de werkprocessen per team gemaakt wordt. Dit is een enorme vooruitgang. Het is soms nog wel zoeken naar de invulling van de rol van ambassadeur, maar door de bijeenkomsten, die naast voorlichting en kennisdeling met name ook een karakter van intervisie hebben, merken de deelnemers vooruitgang.

In november 2024 hebben de privacy ambassadeurs opnieuw meegedaan met de interne auditing.
Voor de meeste ambassadeurs was dit behalve een werksessie ook één grote kennis- en kunde-ervaring.
In november 2025 wordt deze auditsessie opnieuw georganiseerd.
De resultaten van deze interne audit zijn meegenomen in de beoordeling (borgingsproduct 3.0 VNG/IBD), zoals opgenomen in dit jaarverslag.

6. Conclusies

In 2024 heeft de organisatie van de gemeente Nijmegen wederom goede stappen voorwaarts gezet. Maar als FG moet ik ook constateren dat we er nog zeker niet zijn. En dat dit ook niet vanzelf goed komt.
Afgelopen jaar zijn er weer een aantal substantiële vorderingen gemaakt:

1. Eindelijk is het project ‘Mijn Afdeling AVG proof’ afgerond.

2. Waar langzaam de opzet en het bestaan van maatregelen en activiteiten is ingevuld, komt het nu aan om te laten zien dat de werking van naleving van de AVG functioneert. Op dit aspect is nog een forse inspanning te doen.

3. Het opstellen van een risicoscan (in de vorm van DPIA’s) is nog steeds groeiende. Evidenced based aanleveren (aantoonbaar laten zien dat het werkt zoals afgesproken) is groeiende. Naleving van de afspraken uit de DPIA en aanbevelingen uit de beoordelingen, wordt goed opgepakt.

4. Naleving van verwerkersovereenkomsten is matig tot slecht. Hier scoort de organisatie nog onvoldoende.

5. Er zijn verdere stappen gezet op het gebied van privacy protocollen (en de naleving hiervan) voor allerlei samenwerkingsverbanden. Het maken van een overzicht is gestart in 2024 en wordt afgerond in 2025.

6. Ondanks deze stappen in de goede richting, resteert nog steeds een harde constatering: AVG-proof op de volle breedte is de organisatie van de gemeente Nijmegen nog niet.

Bijlagen

1. Tabel Scores Interne Audit

Tabel Scores Interne Audit Stoplichten model
Tijdlijn.
NB voor 2022 en 2023 is Borgingsproduct 2.0 van de VNG/IBD gebruikt. Voor 2024 het nieuwe borgingsproduct 3.0.

Label	Maatregel	Score % 2022	Stoplicht 2022	Score % 2023	Stoplicht 2023	Score % 2024	Stoplicht 2024
1.1.	Algemeen privacy beleid	50	🔴	75	🟠	75	🟠
1.2.	Lijnmanagement verantwoordelijkheden	50	🔴	75	🟠	75	🟠
2.1.	Werkprocessen vaststellen	75	🟠	75	🟠	75	🟠
2.2.	Passende instructies omgang persoonsgegevens	50	🔴	50	🔴	75	🟠
2.3.	Register van verwerkingen	75	🟠	75	🟠	75	🟠
2.4.	Uitvoeren DPIA's	75	🟠	75	🟠	80	🟠
2.5.	Bewaartermijnen	25	🔴	75	🟠	75	🟠
2.6.	Doorgifte buiten EER	75	🟠	75	🟠	75	🟠
2.7.	Privacy eisen wetgeving en contracten	100	🟢	100	🟢	-	-
3.1.	Aanstellen FG	100	🟢	100	🟠	100	🟢
3.2.	Juridische kennis	75	🟠	75	🟠	75	🟠
3.3.	Informeren Ondernemingsraad (OR) en Betrokkenen	100	🟢	100	🟢	75	🟠
3.4.	Middelen voor privacybescherming	50	🔴	75	🟠	75	🟠
4.1.	Processen rechten betrokkenen	75	🟠	75	🟠	75	🟠
4.2.	Geautomatiseerde besluitvorming	100	🟢	100	🟢	50	🔴
4.3.	Informeren Betrokkenen	25	🔴	25	🔴	50	🔴
4.4.	Communicatieplan	25	🔴	25	🔴	50	🔴
4.5.	Privacy- en cookieverklaring	100	🟢	100	🟢	100	🟢
4.6.	Toepassing rechten van betrokkenen	75	🟠	75	🟠	75	🟠
6.1.	Privacy by Design en Privacy By Default	50	🔴	75	🟠	75	🟠
6.2.	Inzicht in privacy incidenten	100	🟢	75	🟠	75	🟠
6.3.	Privacy specifieke beveiligingseisen	100	🟢	100	🟢	75	🟠

NB: Het is haast ondoenlijk om deze tabel te maken. De borgingsproducten 2.0 (2022/2023) en 3.0. (2024) verschillen op de meeste items. De nieuwste versie is op onderdelen uitgebreider met meerdere lagen en meerdere aspecten. Hierdoor kunnen scores lager uitvallen. Daarnaast zijn sommige items niet meer te herleiden. Deze krijgen als score een '-'.
Opname in dit jaaroverzicht is met name bedoeld om een soort tijdlijn te verkrijgen.

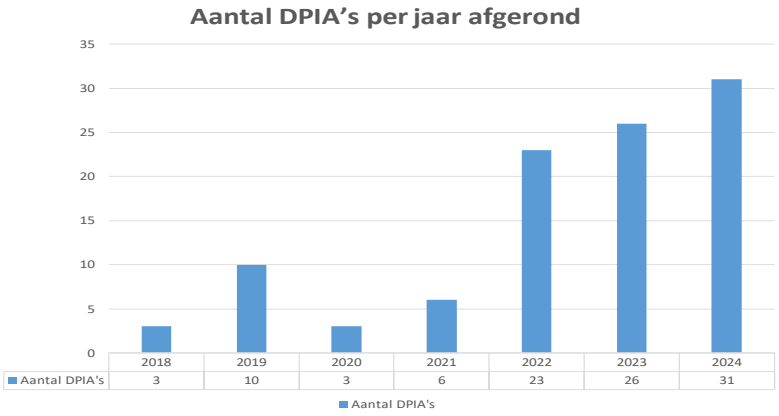
In het jaaroverzicht van 2025 zal alleen nog borgingsproduct 3.0 getoond worden en wordt er een nieuwe tijdlijn opgebouwd vanaf 2024.

Deze informatie is gebaseerd op de registratie in de Cybermanager en de resultaten uit de toetsing 'Controlplan naleving 2024' door de FG.

2. Tabel stand van zaken uitgevoerde DPIA's

Stand van zaken DPIA's per 31/12/24 afgerond	
2018	3
2019	10
2020	3
2021	6
2022	23
2023	26
2024	31
Totaal afgerond	**102**
Onder behandeling per 31/12/24	*40*
Totaal	142

Schematische weergave DPIA's afgerond t/m 2024



3. Duiding ‘Volwassenheidsniveau 3’

Uit bijlage Rekenkamerrapport **“Weten wat je moet weten”.**

Op basis van de geanalyseerde documenten en gevoerde gesprekken hebben de externe onderzoekers een inschatting gemaakt van het volwassenheidsniveau van de gemeenten en iRvN per aandachtsgebied (informatiebeveiliging) en thema (privacybescherming). Volwassenheidsniveau 1 is het laagste en volwassenheidsniveau 5 het hoogste niveau. De onderscheiden niveaus zijn in onderstaande tabel toegelicht.

Niveau	Omschrijving	Indicatieve criteria
1. Ad Hoc	Beheersmaatregelen zijn niet of gedeeltelijk gedefinieerd en/of worden op inconsistente wijze uitgevoerd. Grote afhankelijkheid van individuen.	• Geen of beperkte beheersmaatregelen geïmplementeerd • Niet of ad-hoc uitgevoerd • Niet/deels gedocumenteerd • Wijze van uitvoering afhankelijk van individu
2. Beheerst	Beheermaatregelen zijn aanwezig en worden op consistente en gestructureerde, maar op informele wijze uitgevoerd.	• Beheersmaatregelen zijn geïmplementeerd • Uitvoering is consistent en standaard • Ad-hoc en grotendeels gedocumenteerd
3. Vastgesteld	Beheersmaatregelen zijn gedocumenteerd en worden op gestructureerde en geformaliseerde wijze uitgevoerd. De uitvoering is aantoonbaar en wordt getoetst**.**	• Beheersmaatregel gedefinieerd op basis van risico assessment • Gedocumenteerd en geformaliseerd • Verantwoordelijkheden en taken eenduidig toegewezen • Opzet, bestaan en effectieve werking aantoonbaar • Rapportage van uitvoering van beheersmaatregelen aan management • Effectieve werking van beheersmaatregelen wordt periodiek getoetst, gebaseerd op het risicoprofiel van de organisatie • De toetsing toont aan dat de beheersmaatregel effectief is
4. Voorspelbaar	De effectiviteit van de beheersmaatregelen wordt periodiek geëvalueerd.	• Periodieke (beheersmaatregel) evaluatie en opvolging vindt plaats • Evaluatie is gedocumenteerd en geformaliseerd • Frequentie waarop wordt geëvalueerd is gebaseerd op het risicoprofiel van de organisatie en is minimaal jaarlijks • Rapportage van de evaluatie aan management
5. Geoptimaliseerd	De beheermaatregelen zijn verankerd in het integrale risicomanagement raamwerk, waarbij continu gezocht wordt naar verbetering.	• Continue evalueren van de beheersmaatregelen om de effectiviteit te verbeteren. Gebruik makend van resultaten uit self-assessments, gap- en root cause analyses. • De getroffen beheersmaatregelen worden gebenchmarkt en zijn ‘best practice’ in vergelijking met andere organisaties. • Real time monitoring. • Inzet automated tooling.

4. Duiding gebruikte afkortingen

Afkorting	Duiding
AmvB	Algemene Maatregel van Bestuur
AP	Autoriteit Persoonsgegevens. Zelfstandig bestuursorgaan aangesteld als toezichthouder op het verwerken van persoonsgegevens.
AVG	Algemene verordening gegevensbescherming
Awb	Algemene wet bestuursrecht
BRP	Basisregistratie Personen
B1 taalniveau	Taalniveau B-1 staat voor eenvoudig Nederlands. Een tekst op B-1 niveau bestaat uit makkelijke woorden die iedereen gebruikt.
B&W	Burgemeester en wethouders
CIO	Chief Information Officer: de functionaris die verantwoordelijk is voor de informatievoorziening
CISO	Chief Information Officer: de functionaris die verantwoordelijk is voor het informatiebeveiligingsbeleid
CORSA	Corsa zaakinformatiesysteem. Leverancier is BCT software.
DPIA	Data Protection Impact Assessment: een instrument om vooraf de privacy-risico's van een gegevensverwerking in kaart te brengen.
EER	Europese Economische Ruimte: is het resultaat van een akkoord tussen de Europese Gemeenschap en de Europese Vrijhandelsassociatie.
ENSIA	Eenduidige Normatiek Single Information Audit: verantwoordingsmethodiek voor informatieveiligheid en basisregistraties van gemeenten. Sinds 2017 zijn gemeenten verplicht om jaarlijks een zelfevaluatie in te vullen.
FA	Afdeling Financiën
FG	Functionaris voor de Gegevensbescherming: een functionaris die binnen de organisatie onafhankelijk toezicht houdt op de toepassing en naleving van de Algemene verordening gegevensbescherming (AVG).
GMT	Gemeentelijke Management Team: bestaat uit gemeentesecretaris, directeur en concernmanagers van de gemeente Nijmegen
I	Informatie
IB	Informatiebeveiliging
IBD	Informatie beveiligingsdienst. Deze organisatie is een onderdeel van de VNG (Vereniging van Nederlandse Gemeenten). Meer info: https://www.informatiebeveiligingsdienst.nl/product/avg-borgingsproduct-3-0-documentatie
IRvN	ICT Rijk van Nijmegen. Regionale samenwerkingspartner op ICT-gebied voor de gemeenten in het Rijk van Nijmegen.
IT	Informatie Technologie
KCC	Klant Contact Centrum van de gemeente Nijmegen (onderdeel van de afdeling Publiekszaken)
KPI	Kritieke prestatie indicatoren. Hiermee kunnen de prestaties van een bedrijf, merk of product worden geanalyseerd.
MO	Afdeling Maatschappelijke Ontwikkeling
OR	Ondernemingsraad
PbD	Privacy by Design: gegevensbescherming door ontwerp: tijdens de ontwikkeling wordt rekening gehouden met privacyaspecten.
PIF	Afdeling Personeel, Informatie en Facilitaire zaken
PU	Afdeling Publiekszaken
PvA	Plan van aanpak
SB	Afdeling Stadsbeheer
SR	Afdeling Stadsrealisatie
ST	Afdeling Stadsontwikkeling
SWOT	Analyse van Sterkte (Strengths), Zwakte (Weaknesses), Kansen (Opportunities) en Bedreigingen (Threats).
VJB	Afdeling Veiligheid, Juridische zaken en Bestuursondersteuning
VSA	Afdeling Vastgoed, Sport en Accommodaties
WMO	Wet Maatschappelijke Ondersteuning
Wpg	Wet Politiegegevens: wet regelt de verwerking van persoonsgegevens voor de uitoefening van de politietaak.
VwO	Verwerkersovereenkomst: met een verwerkersovereenkomst sluit de verwerkersverantwoordelijke uit dat de andere partij de persoonsgegevens voor eigen doelen mag verwerken.