

**From:** "5.1.2e" <5.1.2e@nijmegen.nl>  
**Sent:** 2/25/2025 11:09:25 AM  
**To:** "5.1.2e" <5.1.2e@nijmegen.nl>  
**Cc:**  
**Subject:** FW: Jaarverslag FG 2023

---

Voor woe verzoek

---

**Van:** 5.1.2e@nijmegen.nl>  
**Verzonden:** dinsdag 25 juni 2024 14:04  
**Aan:** Astrid van de Klift <a.van.de.klift@nijmegen.nl>  
**CC:** 5.1.2e <5.1.2e@nijmegen.nl>; 5.1.2e <5.1.2e@nijmegen.nl>; 5.1.2e <5.1.2e@nijmegen.nl>;  
<5.1.2e@nijmegen.nl>; 5.1.2e <5.1.2e@nijmegen.nl>  
**Onderwerp:** Jaarverslag FG 2023

Geachte gemeentesecretaris, beste Astrid,

Hierbij stuur ik jou mijn jaarverslag 2023 als functionaris voor de gegevensbescherming (FG) van de gemeente Nijmegen. Samen met 5.1.2e (Privacy Officer) wil ik dit jaarverslag toelichten in een gesprek, welke gepland staat op maandag 1 juli van 13.30 tot 14.00 uur. Dit jaarverslag is inmiddels besproken met de burgemeester en zal ná ons gesprek aangeboden worden aan de wethouder digitalisering. Daarna zal het – conform wens van de Raad – via een collegevoorstel (rondvraagnotitie) aangeboden worden aan de gemeenteraad.

Met vriendelijke groet,

5.1.2e  
Functionaris voor de Gegevensbescherming (FG) gemeente Nijmegen  
Stadscontrol



**Gemeente Nijmegen**  
e-mail: 5.1.2e@nijmegen.nl  
mobiel: 5.1.2e

---

## Jaarrapportage privacy 2023

**Peter Kluver**

Functionaris voor de Gegevensbescherming (FG) gemeente Nijmegen  
Stadscontrol

e-mail: [Functionarisgegevensbescherming@nijmegen.nl](mailto:Functionarisgegevensbescherming@nijmegen.nl)



# Inhoudsopgave

<b>Inhoudsopgave</b>	<b>1</b>
<b>Management samenvatting</b>	<b>2</b>
<b>1. Inleiding</b>	<b>3</b>
<b>2. Stand van zaken privacy binnen de gemeentelijke organisatie</b>	<b>4</b>
2.1 Quick scan Privacy	4
2.2 Uitkomsten interne audit Privacy m.b.v. systeem Cybermanager	6
2.3 Rapportage rekenkameronderzoek informatiebeveiliging en privacy	7
<b>3. Uitvoering Privacy beleid</b>	<b>8</b>
3.1 Privacy beleid update	8
3.2 Rechten van betrokkenen	8
3.3 Incidenten en Datalekmeldingen	8
3.4 Afhandeling Klachten	9
3.5 Onderzoek door of namens de FG	9
<b>4. Check op de naleving op basis van interne controle 2023.</b>	<b>10</b>
4.1 Uitvoering van de plannen van aanpak 'Mijn afdeling privacyproof'	10
4.2 Wpg Audit	11
4.3 DPIA als continu bijstuurproces	11
4.4 Naleving door de organisatie: Inrichting, uitvoering en resultaten controlplan 2023	12
4.5 Privacy Audits	14
4.6 Archivering / vernietiging	14
<b>5. Bewustwording en weerbaarheid</b>	<b>15</b>
5.1 Vergroting I-bewustzijn	15
5.2 Privacy Ambassadeurs	15
<b>Bijlagen</b>	<b>16</b>
1. Tabel Scores Interne Audit	17
2. Tabel stand van zaken uitgevoerde DPIA's	23
3. Duiding 'Volwassenheidsniveau 3'	24
4. Duiding gebruikte afkortingen	25

## Management samenvatting

In 2023 hebben we ('we' is in dit kader: de organisatie van de gemeente Nijmegen) goede stappen voorwaarts gezet. Maar ik moet ook constateren dat we er nog zeker niet zijn. En dat dit ook niet vanzelf goed komt. Afgelopen jaar hebben we een aantal substantiële vorderingen gemaakt: met name op het gebied 'Mijn Afdeling AVG proof' zijn grote stappen gezet. Let wel: nu zijn pas de voorwaarden om te komen tot een 'AVG-proof' organisatie ingevuld. Dat wil nog niet zeggen dat we – volledig – AVG-proof zijn. 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 we langzaam de opzet en bestaan hebben ingevuld, komt het nu aan om het laten zien dat de werking functioneert. Daarmee wordt de lat hoger gelegd en kunnen de kleuren op dát hogere niveau alsnog geel of soms rood geven. We willen toegroeien naar een beheerniveau 3 (uitleg zie bijlage) en daar past deze nieuwe 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 zijn we 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. In 2023 zijn hier extra middelen voor vrij gemaakt. Dit vergt - vooral in het sociaal domein - 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 nog niet de standaard. Evidenced based aanleveren (aantoonbaar laten zien dat het werkt zoals afgesproken) is óók groeiende (er zijn 'best practices'), maar is nog geen gemeengoed. Het is wél de lijn die ik uitdraag als FG. In 2023 zijn er 26 DPIA's opgesteld en voorzien van advies door de FG.

We kennen een sluitende procedure voor wat betreft het opstellen van DPIA's bij nieuwe processen, aanschaf applicaties voor bestaande processen en nieuwe wetgeving. In 2023 is de achterstand op belangrijke processen verder ingelopen: in het sociale domein is een DPIA opgesteld voor de Suite. Het zaakstelsel Corsa kent een DPIA, maar de risico's die hierin benoemd zijn, zijn nog niet allemaal opgelost. Ook zal de DPIA van het personeelsinformatiesysteem begin 2024 afgerond worden.

We kunnen in 2024 stappen gaan maken op het gebied van privacy protocollen (en de naleving hiervan) gebruikt voor allerlei samenwerkingsverbanden. Het volledige overzicht hierop ontbreekt nog.

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.

*Peter Kluver*

*Functionaris voor de Gegevensbescherming Nijmegen*

*April 2024*

# 1. Inleiding

Deze jaarrapportage maakt onderdeel uit van de wettelijke verantwoordingsplicht vanuit de privacywetgeving. 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. Dit jaar heb ik gebruik gemaakt van het format van vorig jaar. Ik kan nu op onderdelen laten zien wat de verschillen zijn tussen 2022 en 2023. 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 niet 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). 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 2023.
- 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 Assessment), 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 2023, 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 weergegeven.

Ons Control systeem ‘Cybermanager’ is inmiddels zo goed als ingericht. Dit is geschiedt op basis van het IBD-borgingsproduct 2.0. Dit is een landelijk vastgestelde normering op het gebied van privacy. Voor de tweede keer hebben we een ‘interne audit’ uitgevoerd op de privacy maatregelen die opgenomen zijn in de Cybermanager. Deze audit is in het vierde kwartaal van 2023 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 het 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) dat is gehouden naar 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 behoudt 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 daar tegen.*

#### **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 2023

### Sterk

- Privacy afspraken: opzet en bestaan
- Privacybeleid (is vastgesteld door de Raad in 2023)
- Leerlijnen via Studytube
- Intake procedure: deze geeft een enorm vangnet en is al effectief gebleken
- PvA Mijn afdeling AVG Proof: geeft een goede analyse en aanpak voor vervolg. Vrijwel alle afdelingen hebben dit afgerond.
- Afhandeling van klachten en incidenten
- 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 vervolgsafspraken: voor de komende drie jaar is er een vervolg ingezet. Ziet er veel belovend uit.
- Interventie op CORSA: 'iedereen lezen' uitgeschakeld en nieuwe autorisatiematrix is ingevoerd. Autorisaties zijn ingedamd.
- De kwaliteit van de beschrijving van de naleving is enorm verbeterd.. Meerdere afdelingen geven uitgebreid en inhoudelijk toelichting hierover.
- Privacybeleid wordt voorzien van KPI's voor meting
- Specifieke aandacht voor privacy in de afdeling.
- Good practise: VSA team privacy en informatiebeveiliging

### 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 matig. 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 contract het einde van het contact met de leverancier.
- Risicomanagement: wel in beeld als belangrijk aspect. Niet geoperationaliseerd.
- Werking van CORSA op het gebied van privacy.
- 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.

### 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.
- Tweede Interne Privacy Audit via Cybermanager: helpt ons in het focussen op de risico's die ertoe doen.
- Privacy ambassadeurs: voor de eerste keer betrokken bij de interne audit
- Ethische Digitale Commissie: eerste advies afgegeven over Datawarehouse.
- Verbeteraanpak CORSA: stap voor stap verbetering.

### Bedreiging

- Implementatie in het Sociale Domein: in 2024 extra middelen beschikbaar (= weer kans)
- Acceptatie van verplichte leerlijnen: blijf zorgen voor duidelijke communicatie over nut en noodzaak, tevens voor budget
- Mijn afdeling AVG Proof: te snelle overdracht en afronding van het traject terwijl een groot deel van de organisatie nog niet de basis heeft gelegd voor een goede aanpak
- Blijvende naleving van de DPIA's. Wordt hopelijk vergroot door toetsing op naleving. Moet niet een eenmalige actie worden,
- Overzicht over de verwerkingsovereenkomsten (uitvraag moet helpen compleet te worden).
- Audits op privacy protocollen: zicht hierop ontbreekt nog. Wordt dit jaar voor het eerst uitgevraagd. In 2024 meer focus op samenwerkingsverbanden.
- Externe factoren zoals cybercriminaliteit, datalekken, technische storingen of andere onvolmaaktheden.



## 2.2 Uitkomsten interne audit Privacy m.b.v. systeem Cybermanager

De inrichting van het registratiesysteem voor informatiebeveiliging en privacy (het systeem Cybermanager) heeft in 2023 een volgend stadium bereikt. Dit door het invoeren van normenkaders voor privacy en het daaraan koppelen van maatregelen om naleving te monitoren. Voor het verkrijgen van inzicht in de risico's die de organisatie loopt op het vlak van informatiebeveiliging en de status van de te treffen maatregelen is het nu nodig dat de afdelingen zelf aan de slag gaan met de risico analyses en de implementatie van maatregelen.

De check op de "in control-maatregelen" (= de onderdelen van het controlplan) vul ik als volgt in:

- Via het systeem Cybermanager kan ik zien welke maatregelen getroffen zijn en welke nog niet. Hier kan een actie uit voortkomen. Dit betreft informatie die voorradig is in het systeem (werkwijze: check melding in systeem en opvolging daarvan).
- Via gerichte vragen nagaan of 'naleving' plaatsvinden oftewel: wordt ook datgene gedaan wat de organisatie afgesproken heeft. Dit gaat met name over houding en gedrag. Dit geschiedt door jaarlijkse uitvoering van het controleplan.

Dit jaar is voor de tweede keer een 'interne audit' uitgevoerd op de maatregelen die opgenomen zijn in de Cybermanager. Deze audit is gedaan door de privacy ambassadeurs, het team informatiebeveiliging en het team privacy. We zijn nu in staat het verschil met 2022 te laten zien. Zo ontwikkelen we langzaam een tijdlijn en wellicht na een aantal jaren een trend.

*Tabel Scores Interne Audit Stoplichten model (in bijlage uitgebreide toelichting)*

Label	Maatregel	Score %	Stoplicht	Score %	Stoplicht
		2022	2022	2023	2023
NL-20.1.1.	Algemeen privacy beleid	50		75	
NL-20.1.2.	Lijnmanagement verantwoordelijkheden	50		75	
NL-20.2.1.	Werkprocessen vaststellen	75		75	
NL-20.2.2.	Passende instructies omgang persoonsgegevens	50		50	
NL-20.2.3.	Register van verwerkingen	75		75	
NL-20.2.4.	Uitvoeren DPIA's	75		75	
NL-20.2.5.	Bewaartermijnen	25		75	
NL-20.2.6.	Doorgifte buiten EER	75		75	
NL-20.2.7.	Privacy eisen wetgeving en contracten	100		100	
NL-20.3.1.	Aanstellen FG	100		100	
NL-20.3.2.	Juridische kennis	75		75	
NL-20.3.3.	Informerend Ondernemingsraad (OR) en Betrokkenen	100		100	
NL-20.3.4.	Middelen voor privacybescherming	50		75	
NL-20.4.1.	Processen rechten betrokkenen	75		75	
NL-20.4.2.	Geautomatiseerde besluitvorming	100		100	
NL-20.4.3.	Informerend Betrokkenen	25		25	
NL-20.4.4.	Communicatieplan	25		25	
NL-20.4.5.	Privacy- en cookieverklaring	100		100	
NL-20.4.6.	Toepassing rechten van betrokkenen	75		75	
NL-20.6.1.	Privacy by Design en Privacy By Default	50		75	
NL-20.6.2.	Inzicht in privacy incidenten	100		75	
NL-20.6.3.	Privacy specifieke beveiligingseisen	100		100	

## 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. Vanuit de analyse en stand van de privacy is dat qua inspanning binnen vier jaar (na 2021) een haalbaar doel, met dien verstande dat er de komende jaren écht nog veel geïnvesteerd dient te worden in de organisatie. Dan hebben we het niet alleen over de middelen, maar ook over wil en oriëntatie, prioritering, kennis en kunde en aansturing.

In onderstaande tabel omschrijven we kort de aanbevelingen die de Rekenkamer gedaan heeft. Daarbij ook de vanuit de organisatie voorgestelde acties (die mede er toe moeten leiden om binnen vier jaar te komen tot dat volwassenheidsniveau 3), inclusief een inschatting van de planning (op kwartalen gebaseerd) voor het aspect privacy.

	Omschrijving aanbeveling rekenkameronderzoek	Voorgestelde actie	Planning
1.	Afspraken tussen gemeenten en IRvN over informatiebeveiliging	CISO	*
2.	Gezamenlijk informatiebeveiligingsbeleid in de regio	CISO	*
3.	Verhelder Beleid informatiebeveiliging en privacybescherming	Er is een update van het strategische Privacy beleid gemaakt. Door College en de Raad vastgesteld medio 2023.	Afgerond
4.	Aanvulling ontbrekende onderdelen beleid	Middels strategisch privacy beleid	Afgerond
5.	Organisatie brede risicoscan	Uitgevoerd door externe organisatie (2023)	Afgerond
6.	Risicomanagement tot continue proces	Eerste inventarisatie en opzet voor vervolg	
7.	Stel voldoende middelen beschikbaar	Er zijn extra middelen beschikbaar of dat voldoende is, moet nog blijken	Besluit in 2023; uitvoering 2024
8.	Geef CISO en FG eigen budget	Niet specifiek bij deze functies belegd; wel bij Stadscontrol	Afgerond
9.	Afspraak over toetsing en rapportage	ENSIA op gebied van beveiliging Interne audit Privacy	Q4 2023
10.	Gebruik KPI's	Als uitvloeisel en onderdeel van strategisch privacy beleid	Q4 2023 Invoering 2024
11.	i-bewustzijn	Doorlopende campagne. Het maakt onderdeel uit van de opgave 'digitale transformatie'	Continue
12.	Meer bestuurlijke aandacht in de gemeente	Griffie	*
13.	Meer bestuurlijke aandacht in de regio	Griffie	*
14.	Vaststellen informatiebeveiliging en privacybeleid in de Raad	Update strategisch privacy beleid	Eind Q2 2023 vastgesteld
15.	Informeren van Raad door bv CISO en FG of externe deskundigen	Middels Raadsbrief; Jaarverslag FG wordt aan College en Raad aangeboden (2023)	Afgerond; speelt elk jaar
16.	Vastleggen controlerende rol	Onderdeel van strategisch privacy beleid	Afgerond
17.	Accountant IT audit	Via Stadscontroller, CISO en CIO	Q1 2023
18.	Regionale aanpak als raden	Keuze Raad	*

\* Items waarbij de verantwoordelijkheid bij anderen is belegd.

## 3. Uitvoering Privacy beleid

### 3.1 Privacy beleid update

In juli 2023 is het nieuwe privacy beleid vastgesteld. Het oude beleid stamde uit 2018 en was toe aan vervanging, gelet op het feit hoe de rol van het thema 'privacy' binnen de gemeente sinds 2018 gegroeid is. Het nieuwe beleid schetst onze 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 wordt de ambitie uitgesproken om binnen vier jaar het volwassenheidsniveau 3 te bereiken.

### 3.2 Rechten van betrokkenen

In 2023 zijn er bij de gemeente 72 verzoeken ingediend. Hier zat één verwijderverzoek bij. De rest waren inzageverzoeken. Het aantal van 72 betreft een behoorlijke stijging ten opzichte van het aantal verzoeken in 2022. De stijging is echter te verklaren doordat middels het AVG inzageproces een groot aantal BRP inzageverzoeken zijn ingediend. De BRP kent echter in de vorm van de Wet BRP een eigen wettelijk kader gericht op inzage in de BRP. Deze verzoeken zijn dan ook doorgezet naar de afdeling Publiekszaken.

Daarnaast hebben meerdere burgers zich rechtstreeks tot de FG gericht middels de functionele e-mailbox [Functionarisgegevensbescherming@nijmegen.nl](mailto:Functionarisgegevensbescherming@nijmegen.nl). Dit betrof veelal vragen om nadere informatie en uitleg over proces en procedures. In 2023 zijn er op deze wijze tien 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.

### 3.3 Incidenten en Datalekmeldingen

In 2023 zijn er 84 beveiligingsincidenten gemeld. Daarvan waren 64 meldingen intern en 20 meldingen extern. Er waren 22 datalekken. Van de datalekken zijn er 13 bij de Autoriteit Persoonsgegevens (AP) gemeld. Over één melding zijn door de AP aanvullende vragen gesteld. Daarbij ging het om 806 stempassen voor de Tweede Kamerverkiezingen. Deze waren verkeerd verstuurd.

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 84 van het afgelopen jaar kunnen we bijvoorbeeld categoriseren naar oorzaak:

Privacy of beveiligingsincident:	47
Verlies / diefstal:	9
Social engineering:	7
Storing beschikbaarheid:	1
Schending privacywetgeving:	7
Datalekken gemeld bij AP:	13

### 3.4. Afhandeling Klachten

In 2023 zijn er in totaal acht 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

Op 13 april 2023 heeft de Autoriteit Persoonsgegevens (AP) bekend gemaakt dat zij voornemens zijn de SVB een boete op te leggen. De AP constateerde dat de SVB een gebrekkige identiteitscontrole uitvoert door de telefonische helpdesk. Uit onderzoek van de AP blijkt dat de SVB te weinig deed om de privacy risico's van de telefonische dienstverlening in kaart te brengen. In de praktijk schoot het systeem voor het controleren van de identiteit van bellers tekort. Controlevragen gingen vaak over zaken die vrij eenvoudig zijn te achterhalen door buitenstaanders (zoals iemands voornaam, adres en postcode). De SVB ging ook onvoldoende na of servicemedewerkers zich eigenlijk wel aan het controlebeleid hielden. De SVB maakte medewerkers onvoldoende bewust van het belang van een veilig beheer van persoonsgegevens.

Deze constatering vanuit de AP richting SVB is voor de FG van de gemeente Nijmegen aanleiding om intern onderzoek te laten doen naar de stand van zaken binnen de gemeentelijke organisatie in het algemeen en het KCC (Publiekszaken) in het bijzonder. Dit onderzoek is uitgevoerd door de Privacy Officer en de Privacy-adviseur.

*Centrale vraag: In hoeverre heeft het KCC voldoende technische en organisatorische maatregelen genomen om de authenticatie en daarmee de informatieveiligheid van het telefonisch contact met burgers te waarborgen?*

Deelvragen:

*1. In hoeverre is een risico- inventarisatie opgesteld waarin specifieke risico's van de verwerking(en) worden geïdentificeerd en gedocumenteerd?*

Een jaar geleden is een DPIA op het proces van het KCC uitgevoerd. De DPIA heeft een aantal risico's in beeld gebracht en de voorgestelde maatregelen om de risico's te mitigeren zijn geïmplementeerd. De komst van het nieuwe KCC-systeem (Tribe) en de bevindingen van de AP zijn aanleiding om de DPIA te actualiseren.

*2. In hoeverre zijn passende beveiligingsmaatregelen opgesteld, gericht op de waarschijnlijkheid van risico's ten aanzien van het telefonisch authenticeren van burgers?*

Een KCC-medewerker is niet bevoegd om op basis van verificatievragen nieuwe informatie vrij te geven waarover telefonisch niet gesproken is met de burger. De KCC-medewerker is enkel bevoegd om informatie die de burger zelf aangeeft te verifiëren.

*3. In hoeverre is er authenticatiebeleid opgesteld met standaard controlevragen en richtlijnen over hoe moet worden omgegaan met situaties waarin twijfel bestaat over de identiteit van de burger?*

De digitale kennisbank vormt de leidraad voor elk klantcontact dat wordt gevoerd door de medewerkers van het KCC. Per onderwerp staan de voorwaarden gerubriceerd die de KCC-medewerker moet uitvoeren c.q. doorlopen. Hier staan ook de verplichte verificatievragen beschreven die de KCC-medewerker moet stellen bij persoonsgebonden vragen. Voor alle nieuwe medewerkers geldt een *verplicht* inwerktraject.

Tenslotte geldt de regel dat het raadplegen van een zaakstelsel altijd persoonsgebonden is. En er daarmee dus verificatievragen gesteld moeten worden, ook bij terugbelnotities.

*4. In hoeverre worden KCC-medewerkers getraind in het authenticatieproces en I-bewust werken?*

Alle medewerkers worden getraind (1x per vier weken) aan de hand van gevoerde gesprekken. Aan de hand van een checklist wordt het gesprek besproken met de medewerker en waar nodig van feedback voorzien. Onderdeel van de checklist vormt de juiste toepassing van de verificatievragen. Hierdoor is er doorlopend aandacht voor het stellen van de verificatievragen en is er steekproefsgewijs controle op het verificatieproces.

## 4. Check op de naleving op basis van interne controle 2023.

### 4.1. Uitvoering van de plannen van aanpak ‘Mijn afdeling privacyproof’

Vrijwel alle afdelingen hebben het traject de “Mijn afdeling AVG-proof” (zo goed als) afgerond. De afdeling IZL is nog druk doende het traject af te ronden. Verwachting is dat dit voorjaar 2024 gebeurd zal zijn.

Succes in deze staat of valt bij de uitvoering door medewerkers in de organisatie. Inrichting van die organisatie kan soms behulpzaam zijn. Bij de uitvraag ‘hielp’ het dat een aantal afdelingen een staforganisatie of een verbijzonderde stafadviseur kennen. Deze afdelingen reageerden over het algemeen op tijd en kwalitatief goed. Andere afdelingen lijken ‘het erbij’ te doen. Dat is eigenlijk ondoenlijk en op termijn risicovol.

Afdeling	2022	2023
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)	●	●

#### Toelichting op Tabel Stoplichtenmodel Mijn afdeling Privacyproof

Rood: Processen nog niet volledig in beeld, niet alle bureaus aangesloten. Oranje: P.v.A. gereed, processen deels in beeld, eerste risicoscan gemaakt. Groen: processen in beeld, risicoscan gemaakt, alle bureaus afgerond, overdrachtsdocument ingeleverd bij FG.

Afronding van het traject betekent nog niet dat de afdelingen ook daadwerkelijk AVG proof zijn. De eerste stap is gemaakt. In de trits ‘opzet – bestaan – werking’ is de eerste fase afgerond. ‘Opzet’: De processen zijn in beeld, er is duidelijk wat er moet gebeuren en deze acties zijn ingepland. ‘Bestaan’ betekent dat er ook uitvoering aan gegeven wordt. Er zijn medewerkers die zich hiermee bezighouden conform planning. ‘Werking’ betekent dat ‘evidenced based’ de organisatie laat zien op welke wijze ze de acties heeft uitgevoerd en zich gehouden heeft aan de afspraken en normeringen. Om een idee te geven hoe dat eruit ziet, geef ik een overzicht per afdeling op basis van een eerste *inschatting* van de overdrachtsdocumenten, die de afdelingen hebben gegeven.

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)	●	●	●

Nb. De rode stip bij MO betreft het ontbreken van informatie over naleving DPIA's en verwerkersovereenkomsten.

## 4.2. Wpg Audit

In 2022 heeft de (verplichte) externe audit op naleving van de Wet Politiegegevens (Wpg) plaatsgevonden. Voorjaar 2023 hebben we hierop een (externe) hercontrole gehad 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 hebben we als 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.

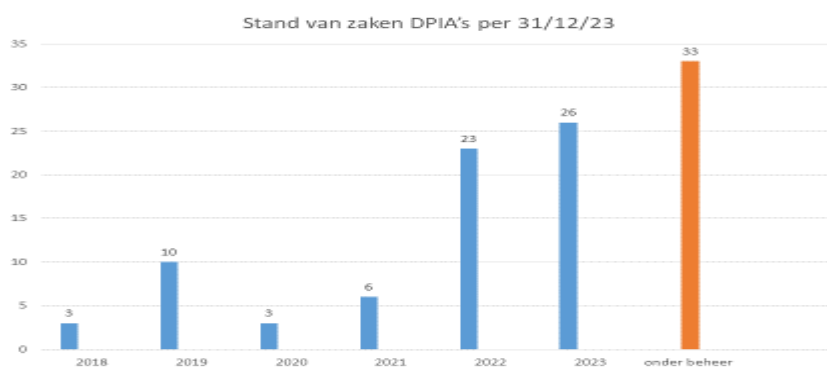
In het najaar 2022 is er reeds een interne (tweede) audit geweest op dit domein door een interne auditeur, die hiervoor in de organisatie benoemd is. Hier werden reeds de eerste vorderingen opgemerkt.

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.

## 4.3. DPIA als continu bijstuurproces

Het instrument DPIA is nog steeds teveel 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 2023 zijn in totaal 26 DPIA's uitgevoerd op grote complexe gegevens verwerkingen binnen het fysiek, sociaal en veiligheidsdomein. In de jaarlijkse controle wordt getoetst in hoeverre uitvoering en borging wordt gegeven aan de risico's en maatregelen zoals opgenomen in de DPIA's.



#### 4.4. Naleving door de organisatie: Inrichting, uitvoering en resultaten controlplan 2023

In het najaar 2023 heeft de Functionaris voor de gegevensbescherming, zoals inmiddels gebruikelijk, een interne controle uitgevoerd op naleving van de AVG door de gemeentelijke organisatie. Object van onderzoek was:

- Voortgang 'Mijn afdeling AVG-proof';
- Registraties datalekken, klachten en incidenten zoals opgenomen in de Cybermanager;
- Naleving van afspraken gemaakt in de DPIA en in de beoordelingen daarvan;
- Naleving van privacy protocollen
- Naleving van de afspraken gemaakt in verwerkersovereenkomsten.

Ondanks dat er grote stappen zijn gezet op het vergroten van het informatiebewustzijn en het werken conform de AVG zijn er een viertal belangrijke constatering op te maken:

- Er is voortgang op het traject mijn afdeling AVG-proof. Inmiddels hebben vrijwel alle afdelingen (van de 10) dit traject afgerond. Eén deling nadert de afronding.
- Naleving van de DPIA's gaat al beter dan voorgaande jaren. Evidenced based aanleveren (aantoonbaar laten zien dat het werkt zoals afgesproken) is nog geen gemeengoed. Opgemerkt dient te worden dat de kwaliteit van de beschrijving van de naleving enorm verbeterd is. Meerdere afdelingen geven uitgebreid en inhoudelijk toelichting hierover. Dat is een goede stap voorwaarts!
- De uitvoering van verwerkersovereenkomsten wordt onvoldoende getoetst op naleving bij leveranciers. Bij navraag vanuit de toezichthoudende rol gebeurt dit wél als resultante van de hercontrole, echter als regulier onderdeel van de normale bedrijfsvoering is dit géén gemeengoed.
- Er is nu een betere inventarisatie van de aanwezigheid van privacy protocollen in de organisatie, maar er is nog geen geheel overzicht. Naleving staat nog in de kinderschoenen.

#### Tafel van Elf

De resultaten uit het controlplan 2023 geven we weer in onderstaande tabel. Daarbij hebben we gebruik gemaakt van de 'Tafel van Elf', ontwikkeld door het ministerie van Justitie en 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 (zoals een wet) 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 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 in de afdelingen. Nóg meer gebruik van maken.
	Normgetrouwheid doelgroep	Middel tot hoog	Middel	Hier spelen de privacy ambassadeurs een rol. Die kan verder uitgewerkt worden
	Niet overheidscontrole: Sociale controle / horizontaal toezicht	Middel	Middel	Niet ingezet Sociale controle: afwezen. Impliciet via de privacy ambassadeurs. Horizontaal toezicht: inbedden.
Handhaving				
	Meldingskans	Laag	Laag	Kan voorkomen via externe melding (burger, instantie of AP); (nog) niet voorgekomen.
	Controlekans	Laag	Middel, wordt hoger	Deze is verhoogd en geeft effect. Aanlevering is zowel in tijd als kwaliteit beter dan in 2022. Control uitvraag wordt ingepland in P&C cyclus.
	Detectiekans	Laag	Laag tot middel	Verwerkersovereenkomsten derde steekproef; In 2024 wordt deze uitgebreid naar alle overeenkomsten. DPIA's worden allen op naleving getoetst. De detectiekans is dan 100%.
	Selectiviteit	Laag	Laag	We onderscheiden via 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.

## 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.

De naleving van (overeengekomen en vastgelegde) afspraken uit de diverse verwerkersovereenkomsten is teleurstellend te noemen. In 2024 willen we het gehele register laten checken op naleving. We willen alle verwerkingen met mogelijk hoog risico waarin met persoonsgegevens wordt gewerkt, in de komende jaren van een DPIA voorzien. Wij hanteren hierbij het Register van Verwerkingen als basis. Wij realiseren ons dat dit een grote opgave is (en tevens een inhaalslag is).



## 4.5. Privacy Audits

Op basis van artikel 31 van het privacy protocol “Zorg- en Veiligheidshuis Gelderland Zuid” is medio 2022 een interne audit uitgevoerd naar de opzet, het bestaan en de werking van het Privacy Protocol Veiligheidshuis Gelderland Zuid (hierna: protocol). De naleving van het protocol behoort door partijen tweejaarlijks te worden getoetst. Op deze wijze kan aantoonbaar worden voldaan aan de verantwoordingsplicht zoals opgenomen in de AVG. Eerste obstakel in deze oordeelsvorming was het ontbreken van een DPIA op de gegevensverwerking. In 2023 is deze DPIA afgerond. Andere maatregelen uit de audit zijn geïmplementeerd.

## 4.6. Archivering / vernietiging

In 2022 en ook in 2023 heeft één project expliciete en intensieve aandacht van de FG gehad. Dit betreft het project Corsa AVG-proof. Corsa is het algehele zaakstelsel 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 stelsel kreeg, ook alles kon zien. Dit was vanuit privacy overwegingen onaanvaardbaar. Vandaar dat de FG op dit dossier nadrukkelijk heeft geadviseerd. Mede hierdoor heeft het project Corsa AVG-proof in 2022 een extra versnelling gekregen.

Een groot privacy probleem in Corsa is (uiteindelijk) verholpen door een andere benadering te kiezen. 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. Hiervoor is een autorisatiematrix gemaakt die in 2023 ingevoerd is.

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.

Verder ontbreekt door de decentrale opzet nog steeds een generiek beeld van de naleving van bewaartermijn. Dit kwam ook terug uit de bevindingen van de Archiefinspectie (2022) met betrekking tot digitale vernietiging.

## 5. Bewustwording en weerbaarheid

### 5.1. Vergroting I-bewustzijn

Op het gebied van bewustwording heeft in 2019 én in 2022 een ‘mystery visit’ plaatsgevonden. Hier zijn een aantal verbeterpunten uit naar voren gekomen. Die hebben wij in 2020 en 2022 geïmplementeerd. Dit heeft onder andere geleid tot een voorstel tot het benoemen van i-bewustzijn als belangrijk thema voor de Nijmegen School in 2022. In de digitale opleidingsmodule zijn verplichte leerlijnen over Privacy en Informatiebeveiliging opgenomen voor alle medewerkers. De uitkomsten van deze actie worden meegenomen in het opleidingsprogramma. Dit heeft (mede) geleid tot de implementatie van een wachtwoordmanager en mobile device management.

In 2023 is het Gedragsteam Nijmegen van Nu opgericht. Dat is een team waarin verschillende expertises (communicatie, gedrag, P&O, privacy, informatiebeveiliging, dienstverlening) samen zijn gebracht. Dit team zorgt voor gecoördineerde interventies, onder andere op het vlak van privacy en informatiebeveiliging. Verder is in 2023 de leerlijn ‘ransomware’ verplicht gesteld aan al onze medewerkers.

### 5.2. Privacy Ambassadeurs

In 2023 hebben we twee bijeenkomsten gehad met de groep privacy ambassadeurs. Deze groep is gegroeid. Hadden de afdelingen in 2022 meestal één of twee ambassadeurs, nu heeft bijna elk team / bureau een ambassadeur. In het totaal kent de gemeentelijke organisatie op dit moment 44 ambassadeurs. Afspraak is dat elk bureau in een afdeling minimaal één ambassadeur dient te hebben.

Dit betekent dat we hiermee directer een verbinding met de werkprocessen per team kunnen maken. 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 we dat we hierop vooruitgang boeken als organisatie.

In november 2023 hebben de privacy ambassadeurs meegedaan met de interne auditing. Voor de meeste ambassadeurs was dit behalve een werksessie ook één grote kennis- en kunde-ervaring.

In november 2024 willen we deze auditsessie opnieuw organiseren.

De resultaten van deze interne audit zijn meegenomen in de beoordeling, zoals opgenomen in dit jaarverslag.

## Bijlagen

**23 november 2023 met privacy ambassadeurs en 4 december 2023 met experts**

17

Label	Maatregel	Audit instructie	Score %	Verklaring	Stoplicht
		voor medewerkers over de omgang met persoonsgegevens in werkprocessen en worden ze daarop getraind? Zijn er passende instructies en protocollen voor hoog risicoverwerkingen		Voor specifieke werkprocessen is deze (nog) niet volledig ontwikkeld. Privacyprotocollen kennen een eigen format.	
NL-20.2.3.	Register van verwerkingen	Is er een gedocumenteerd verwerkingsregister die organisatie breed inzicht geeft in verwerkingen van de gemeente en is het beheer intern belegd? Is er een gedocumenteerd register van verwerkingen?	75	2022: Ja er is een register van verwerkingen. Er ontbreekt een procesbeschrijving met betrekking tot het vullen, actualiseren en toezien op het register.  2023 (in samenspraak met privacy ambassadeurs): Opzet: 100; Bestaan: 100; Werking: 75. Vanuit het perspectief van de afdelingen: De meeste hebben dit op orde. Sommige zijn bezig met een inhaalslag. Dat betekent op het geheel dat we niet zeker weten of we alles in beeld hebben.	  
NL-20.2.4.	Uitvoeren DPIA's	Worden DPIA's structureel uitgevoerd en mitigerende maatregelen doorgevoerd door de proceseigenaren? Worden DPIA's structureel uitgevoerd en mitigerende maatregelen doorgevoerd	75	2022: Ja, er worden voor nieuwe wetten, nieuwe processen en nieuwe systemen DPIA's uitgevoerd. Maatregelen vanuit die DPIA's worden uitgevoerd en doorgevoerd. Hierop wordt eens per jaar getoetst. Nog niet voor alle bestaande processen en de daarbij bijpassende systemen is een DPIA uitgevoerd. In 2022 is en start gemaakt deze achterstand in te halen.  2023 (in samenspraak met privacy ambassadeurs): Opzet: 100; Bestaan: 100; Werking: 75. Privacy ambassadeurs geven aan dat ze wel bekend zijn met DPIA's op de afdeling. Graag willen zij hierover meer informatie ontvangen. Het aantal DPIA's dat gemaakt wordt is nu steeds stijgende. De Raad heeft het aantal beoordeelde DPIA's als KPI opgenomen.	  
NL-20.2.5.	Bewaartermijnen	Worden persoonsgegevens die niet meer nodig zijn tijdig verwijderd of geanonimiseerd? Worden persoonsgegevens tijdig vernietigd?	25  75	2022: Dit gebeurt nog niet voldoende. Is wel onderdeel van vele projecten (Corsa, digitalisering etc), maar nog niet structureel ingebed. Overzicht ontbreekt waar dit wél en níet gebeurt.  2023 (in samenspraak met privacy ambassadeurs): Opzet 100; Bestaan: 100; Werking: 50 Organisatie is bezig met een grote inhaalslag. Suite wordt opgeschoond. Dit geldt ook voor Corsa. Ook in andere processen wordt hier aan gewerkt.	  

Label	Maatregel	Audit instructie	Score %	Verklaring	Stoplicht
				In generieke zin is er meer aandacht middels de verplichte leerlijnen die gevolgd moeten worden.	
NL-20.2.6.	Doorgifte buiten EER	Zijn doorgiften van persoonsgegevens naar derde landen en internationale organisaties - en de bijbehorende transfermechanismen - bekend respectievelijk getoetst? Verwerkingen met doorgifte buiten de EER zijn in beeld?	75	<p>2022:</p> <p>De werkwijze rondom het opslaan van data buiten de EER zijn bekend bij alle specialisten, maar allicht niet gemeente breed. Er is altijd aandacht voor in DPIA's en intakes waar de data wordt opgeslagen. Daarnaast hebben we een stroomschema opgesteld waarin onze uitgangspunten met betrekking tot het kiezen van de locatie waar we onze data opslaan hebben vastgelegd. Als er een passend alternatief is om data op te slaan binnen de EER in plaats van er buiten, pakken we die. Als dat niet zo is, voldoen we aan de aanvullende maatregelen die vereist zijn.</p> <p>2023: Geen aanpassingen</p>	
NL-20.2.7.	Privacy eisen wetgeving en contracten	<p>Zijn sancties in wetgeving en contracten en contractuele eisen over de bescherming van persoonsgegevens bekend?</p> <p>Zijn sancties zoals opgenomen in verwerkersovereenkomsten en vastgesteld door de Autoriteit inzichtelijk</p>	100	<p>2022:</p> <p>Er zijn twee templates verwerkers-overeenkomsten. In het IBD model VwO zijn geen sanctiemaatregelen opgenomen. Dit model vormt het uitgangspunt bij het vastleggen van een verwerking tussen de verantwoordelijke en de verwerker (pas toe of leg uit). Daarnaast is er een eigen gemeentelijk model voor het geval er geen voorwaarden of hoofdovereenkomst van toepassing is. Hierin zijn wel sanctiemaatregelen opgenomen. Sancties en de sanctiematrix van de AP zijn bij AmvB vastgesteld.</p> <p>2023: Geen aanpassingen</p>	
NL-20.3.1.	Aanstellen FG	<p>Zijn de taken van de FG duidelijk omschreven, de rol goed gepositioneerd in de organisatie en worden de adviezen van de FG opgevolgd, althans gemotiveerd beantwoord?</p> <p>Is er een FG aangesteld en is deze goed gepositioneerd in de organisatie?</p> <p>Worden de adviezen van de FG opgevolgd? Zo niet, worden de adviezen van een gemotiveerd antwoord voorzien.</p>	100	<p>2022:</p> <p>Ja, de rol van FG is door het college vastgesteld. Ja, de adviezen worden opgevolgd door het college. De positie ligt vast bij een derde lijn afdeling. De onafhankelijkheid is geborgd middels een addendum op de aanstelling.</p> <p>2023: Geen wijzigingen.</p>	
NL-20.3.2.	Juridische kennis	Is er voldoende kennis en kunde aanwezig binnen de organisatie op het gebied van Privacy?	75	<p>2022:</p> <p>Bij de specialisten is voldoende vakinhoudelijke kennis aanwezig. Dit is geborgd in het kenniscluster privacy en Informatieveiligheid. Binnen de vakafdelingen wordt kennis en kunde gemeten met</p>	



Label	Maatregel	Audit instructie	Score %	Verklaring	Stoplicht
		Zijn er processen ingericht om de rechten van betrokkenen te faciliteren? Verdergaande mogelijkheden om invulling te geven aan de rechten van betrokkenen worden toegepast?		<p>wij uitleg over het gebruikmaken van de Rechten van Betrokkenen. Dit document is in B1 taalniveau opgesteld.</p> <p>Ja, er is een privacyportal beschikbaar via de website van de gemeente Nijmegen. Dit portal is gekoppeld aan bovengenoemde procedure. Verdergaande mogelijkheden om invulling te geven aan de rechten van betrokkenen worden toegepast. Waar mogelijk worden applicaties privacy by design ingericht. Hier maakt de borging van de rechten van betrokkenen onderdeel van uit.</p> <p>2023: Procedure is efficiënter ingericht Opzet 100; Bestaan 100; Werking 75 Het proces werkt, maar we kunnen nog niet 100% garanderen dat alles gaat zoals het bedoeld is. Ook deze indicator is door de Raad als KPI aangewezen.</p>	
NL-20.4.2.	Geautomatiseerde besluitvorming	<p>Is organisatie breed bekend wanneer geautomatiseerde besluitvorming wordt toegepast en worden daarbij passende privacy waarborgen getroffen?</p> <p>Is er inzichtelijk welke besluiten genomen zijn op basis van automatisch verwerkte persoonsgegevens?</p>	100	<p>2022: Ja, dit om te voorkomen dat de menselijke tussenkomst wordt overgeslagen. Dit conform het door de raad vastgestelde Manifest Open en Weerbaar Nijmegen uit 2017. Er worden geen besluiten genomen zonder tussenkomst van een ambtenaar.</p> <p>2023: Geen aanpassingen</p>	
NL-20.4.3.	Informeren Betrokkenen	<p>Worden betrokkenen tijdig en adequaat geïnformeerd over verwerkingen van hun persoonsgegevens volgens de transparantieverplichtingen?</p> <p>Worden betrokkenen actief, tijdig en adequaat geïnformeerd?</p>	25	<p>2022: Nee, we doen dit alleen globaal via de privacyverklaring. Betrokkenen worden actief, tijdig en adequaat geïnformeerd. Nee, alleen globaal via de privacyverklaring op de website van de gemeente Nijmegen.</p> <p>2023: geen aanpassingen. In 2024 wordt bekeken of er meer actief gecommuniceerd kan worden bij het starten van een proces / procedure.</p>	
NL-20.4.4.	Communicatieplan	<p>Is er een organisatie breed communicatieplan over privacy waarin structureel rekening wordt gehouden met transparantieverplichtingen?</p> <p>Is er een communicatieplan over privacy gericht op een invulling aan de AVG-transparantieverplichtingen?</p>	25	<p>2022: Het communicatieplan gaat niet op het borgen van transparantie-verplichtingen. Nee er is geen communicatieplan op specifieke gegevensverwerkingen waar transparantieverplichtingen op van toepassing zijn.</p> <p>2023:</p>	

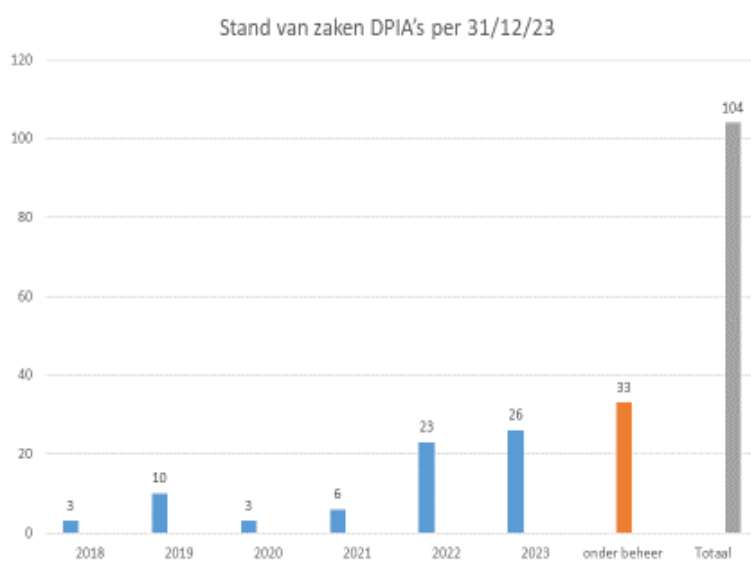


Label	Maatregel	Audit instructie	Score %	Verklaring	Stoplicht
				We communiceren over privacy middels onze privacyverklaring. Wat we beter zouden kunnen doen is om bij bijvoorbeeld een aanvraagformulier het verwerkingsdoel van de gegevens aangeven. Daarnaast wordt 'Mijn Nijmegen' doorontwikkeld en dat geeft ook meer inzichten. Opzet 50; Bestaan 50; Werking: 25	
NL-20.4.5.	Privacy- en cookieverklaring	Zijn de privacy- en cookieverklaring actueel en geven ze gemeente breed inzicht in verwerkingen van persoonsgegevens door de gemeente?  Staat op de gemeentelijke website een privacy- en cookieverklaring met informatie over verwerkingen van persoonsgegevens door de gemeente?	100	2022: Ja, de privacyverklaring is actueel. De verklaring verwijst naar het register waar inzicht kan worden verkregen over alle verwerkingen. De verklaring geeft alleen op hoofdlijnen uitleg. Op de gemeentelijke website staat een privacy- en cookieverklaring met informatie over verwerkingen van persoonsgegevens door de gemeente.  2023: Geactualiseerd.	
NL-20.4.6.	Toepassing rechten van betrokkenen	Worden verdergaande mogelijkheden toegepast om invulling te geven aan de rechten van betrokkenen?	75	2022: Zie vraag rechten van betrokkenen.  2023: zie 20.4.3.	
NL-20.6.1.	Privacy by Design en Privacy By Default	Wordt rekening gehouden met PbD en privacy by default bij (potentieel) nieuwe verwerkingen?  Worden verwerkingen zodanig ingericht dat rekening wordt gehouden met de acht beginselen van Privacy by Design (PbD) en privacy by default?	50  75	2022: Ja, hier wordt rekening mee gehouden via het intake en inkoopproces. Echter er is geen borging met betrekking tot het structureel borgen van de uitvraag en werking van Privacy by Design. Ja, waar mogelijk. Alleen is dit niet consequent geborgd en vastgelegd.  2023 (in samenspraak met privacy ambassadeurs): Privacy ambassadeurs geven aan dat bij de aanbestedingen rekening gehouden wordt met principe van Privacy by Design. Privacy by Default is verschillend per afdeling. Dit vormt wel het uitgangspunt. Opzet 100; Bestaan 100; Werking 50	  
NL-20.6.2.	Inzicht in privacy incidenten	Is incidentbeheer ingericht met gedocumenteerde procedures voor het behandelen van privacy-incidenten en weten medewerkers hoe ze op een incident moeten reageren?  Heeft de gemeente inzicht in (potentiële) privacy-incidenten, zoals datalekken?	100  75	2022: Ja, er is een gemeentelijke procedure. Deze is echter niet vastgesteld in het college. Het maakt onderdeel uit van de elearning op privacy en informatieveiligheid. Het maakt tevens onderdeel uit van het inwerkprogramma. Ja, hiervoor wordt een register bijgehouden.  2023 (in samenspraak met privacy ambassadeurs): Opzet: 100; Bestaan: 100; Werking: 75. Privacy ambassadeurs geven aan dat er aandacht is voor datalekken en incidenten. Op een paar afdelingen is dit minder. Score Volledigheid	  

Label	Maatregel	Audit instructie	Score %	Verklaring	Stoplicht
				Score Juistheid	●
NL-20.6.3.	Privacy specifieke beveiligingseisen	Houdt het IB-beleid en de IB-procedures rekening met privacy specifieke beveiligingseisen?  Houdt het IB-beleid rekening met privacy specifieke beveiligingseisen?	100	Ja, de privacyspecifieke beveiligingseisen maken nadrukkelijk onderdeel uit van het IB beleid.  Ja, er is een nadrukkelijke koppeling met het privacybeleid. Daarnaast maakt privacy onderdeel uit van de jaarlijkse ENSIA rapportage.  2023: Geen aanpassingen	●

## 2. Tabel stand van zaken uitgevoerde DPIA's

Stand van zaken DPIA's per 31/12/23 afgerond	
2018	3
2019	10
2020	3
2021	6
2022	23
2023	26
<b>Totaal afgerond</b>	<b>71</b>
Onder behandeling per 31/12/23	33
<b>Totaal</b>	<b>104</b>



### 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.	<ul style="list-style-type: none"> <li>• Geen of beperkte beheersmaatregelen geïmplementeerd</li> <li>• Niet of ad-hoc uitgevoerd</li> <li>• Niet/deels gedocumenteerd</li> <li>• Wijze van uitvoering afhankelijk van individu</li> </ul>
2. Beheerst	Beheersmaatregelen zijn aanwezig en worden op consistente en gestructureerde, maar op informele wijze uitgevoerd.	<ul style="list-style-type: none"> <li>• Beheersmaatregelen zijn geïmplementeerd</li> <li>• Uitvoering is consistent en standaard</li> <li>• Ad-hoc en grotendeels gedocumenteerd</li> </ul>
3. Vastgesteld	Beheersmaatregelen zijn gedocumenteerd en worden op gestructureerde en geformaliseerde wijze uitgevoerd. De uitvoering is aantoonbaar en wordt getoetst.	<ul style="list-style-type: none"> <li>• Beheersmaatregel gedefinieerd op basis van risico assessment</li> <li>• Gedocumenteerd en geformaliseerd</li> <li>• Verantwoordelijkheden en taken eenduidig toegewezen</li> <li>• Opzet, bestaan en effectieve werking aantoonbaar</li> <li>• Rapportage van uitvoering van beheersmaatregelen aan management</li> <li>• Effectieve werking van beheersmaatregelen wordt periodiek getoetst, gebaseerd op het risicoprofiel van de organisatie</li> <li>• De toetsing toont aan dat de beheersmaatregel effectief is</li> </ul>
4. Voorspelbaar	De effectiviteit van de beheersmaatregelen wordt periodiek geëvalueerd.	<ul style="list-style-type: none"> <li>• Periodieke (beheersmaatregel) evaluatie en opvolging vindt plaats</li> <li>• Evaluatie is gedocumenteerd en geformaliseerd</li> <li>• Frequentie waarop wordt geëvalueerd is gebaseerd op het risicoprofiel van de organisatie en is minimaal jaarlijks</li> <li>• Rapportage van de evaluatie aan management</li> </ul>
5. Geoptimaliseerd	De beheersmaatregelen zijn verankerd in het integrale risicomanagement raamwerk, waarbij continu gezocht wordt naar verbetering.	<ul style="list-style-type: none"> <li>• Continue evalueren van de beheersmaatregelen om de effectiviteit te verbeteren. Gebruik makend van resultaten uit self-assessments, gap- en root cause analyses.</li> <li>• De getroffen beheersmaatregelen worden gebenchmarkt en zijn ‘best practice’ in vergelijking met andere organisaties.</li> <li>• Real time monitoring.</li> <li>• Inzet automated tooling.</li> </ul>

## 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)
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.
Log4J	Een op JAVA (computertaal) gebaseerd hulpprogramma voor logboekregistratie
MO	Afdeling Maatschappelijke Ontwikkeling
OR	Ondernemingsraad
PbD	Privacy by Design: gegevensbescherming door ontwerp: tijdens de ontwikkeling van producten en diensten 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.

# Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1