

Rapportage Uitvoering Controlplan FG 2023

Peter Kluver

Functionaris voor de Gegevensbescherming (FG) gemeente Nijmegen
Stadscontrol

e-mail: Functionarisgegevensbescherming@nijmegen.nl

Versie 1.0 19/03/24/PK

Uitvoering controlplan FG 2023: Bevindingen naleving

Inleiding

Eind 2023 heeft de stuurgroep AVG de opzet en planning van het controlplan van de FG van de gemeente Nijmegen besproken en vastgesteld. Deze control betreft een vijftal stappen:

1. Bevindingen traject “Mijn afdeling AVG proof”;
2. Bevindingen incidenten en datalekmeldingen jaarschijf 2023;
3. Bevindingen control op naleving DPIA’s vastgesteld in de periode zomer 2022 – najaar 2023 (vervaldatum 15/10/23); vervolg op de rapportages naleving DPIA’s vastgesteld vóór zomer 2022.
4. Bevindingen control op naleving Verwerkersovereenkomsten (vwo’s) middels een nieuwe steekproef van 10 vwo’s en vervolgrapportages op bevindingen controlplan 2021 én 2022.
5. Bevindingen naleving privacy protocollen.

In deze rapportage wordt de naleving van de gemaakte afspraken beschreven. Per hoofdstuk wordt kort en soms ondersteund middels een stoplichtenmodel aangegeven hoe de organisatie deze naleving heeft uitgevoerd.

In de bijlagen wordt gedetailleerder ingegaan op de opgehaalde uitkomsten.

Middels toepassing van de tafel van 11 (uitleg zie h6.) wordt schematisch aangegeven per dimensie op welk niveau de organisatie de naleving heeft vormgegeven en welke aanbevelingen en mogelijke acties te doen zijn om dit te verbeteren. Daarna volgen de conclusies en aanbevelingen gericht aan het management van de organisatie vertegenwoordigd in het GMT.

Management samenvatting / conclusies

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:

- Het traject mijn afdeling AVG-proof kan afgerond worden. Dit wil niet zeggen dat de afdelingen AVG-proof zijn. Wél dat alle afdelingen een scan hebben gemaakt en daarmee inzicht hebben in welke acties nog ondernomen moeten worden. De voorwaarden voor het AVG-proof werken zijn daarmee geschapen. Komende jaren gaan we een beweging maken van opzet, naar bestaan en tenslotte naar werking (conform beheer niveau 3). Met het afronden van het traject is ‘opzet’ gereedgekomen. Nu volgen nog de stappen ‘bestaan’ en ‘werking’. Hierop zal de toetsing van 2024 zich richten.
- Naleving van de DPIA’s gaat al beter dan voorgaande jaren. Evidence based aanleveren (aantoonbaar laten zien dat het werkt zoals afgesproken) is nog geen gemeengoed. IZL heeft hierin goede voorbeelden laten zien. Andere afdelingen zouden hier gebruik van kunnen maken.
- De uitvoering van verwerkersovereenkomsten wordt (nog steeds) onvoldoende getoetst op naleving. Dit is teleurstellend te noemen. In 2024 willen we het gehele register laten checken op naleving.
- Privacy protocollen in de organisatie blijven nog steeds onderbelicht. We krijgen langzaam een beter beeld, maar een algemeen overzicht ontbreekt nog.

Wat mij opvalt is dat deze conclusies enigszins gelijk zijn aan die van voorgaande jaren (2021 en 2022).

Is de organisatie dan niet verbeterd en zijn er dan geen resultaten geboekt?

Dat is in 2023 zeker wel gebeurd. Veel afdelingen hebben forse stappen voorwaarts gezet, zeker op het niveau mijn afdeling AVG-proof en bij het oppakken van DPIA’s. We zijn écht op pad om - in ‘stoplicht termen’ - van rood, naar geel, naar groen te gaan. Alleen is óók geel nog niet groen....

En om dat te bereiken moet - nog steeds - veel effort geleverd worden.

1. Bevindingen traject 'Mijn afdeling AVG proof'

Er is voortgang op het traject mijn afdeling AVG-proof. In dit traject dienen de afdelingen hun processen door te lichten op privacyaspecten en te komen met maatregelen om de privacy te waarborgen. Inmiddels hebben negen afdelingen (van de 10) dit traject (vrijwel) afgerond. De laatste afdeling is goed op weg en nadert de afronding. Verwachting is dat deze in het voorjaar 2024 het traject zal afronden.




Tabel Stoplichtenmodel Mijn afdeling Privacyproof

Rood: Plan van Aanpak (P.v.A.) wel/niet gereed, processen nog niet volledig in beeld, nog niet alle bureaus aangesloten.

Oranje: P.v.A. gereed, processen deels in beeld, eerste risicoscan gemaakt, nog niet afgerond, deel bureaus gereed, anderen begonnen.

Groen: processen in beeld, volledige risicoscan gemaakt, alle bureaus afgerond, overdrachtsdocument (zo goed als) ingeleverd bij FG.

Stand per jan 2024

			
Afdeling		Inkomen, Zorg en Leerrecht (IZL)	Financiën (FA); 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)































Verloop:

Medio 2022 zijn de afdelingen begonnen om de uitvoering van het "Mijn afdeling AVG-proof" plan weer op te pakken, na stilstand door de Coronapandemie. Vrijwel alle afdelingen hebben dit traject (zo goed als) afgerond. De afdeling IZL is nog drukdoende het traject af te ronden.

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 en de eerste fase van 'het bestaan'. De processen zijn in beeld, er is duidelijk wat er (nog) moet gebeuren en deze acties zijn ingepland. In 2024 zal die planning gevolgd worden (de handelingen rondom het 'bestaan': het vaststellen dat maatregelen werken zoals beschreven) en zullen de acties beoordeeld worden (volgen van de 'werking' en naleving van de opzet).

Om vast een idee te geven hoe dat er uit gaat zien, zal ik een overzicht geven per afdeling op basis van een eerste inschatting van de overdrachtsdocumenten die de afdelingen hebben aangeleverd.

Stand per jan 2024 (inschatting)

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.

2. Bevindingen incidenten, klachten en datalekmeldingen jaarschijf 2023

2.1. Afhandeling klachten

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. 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.

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.

2.2. 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 een 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
Kwetsbaarheid	13

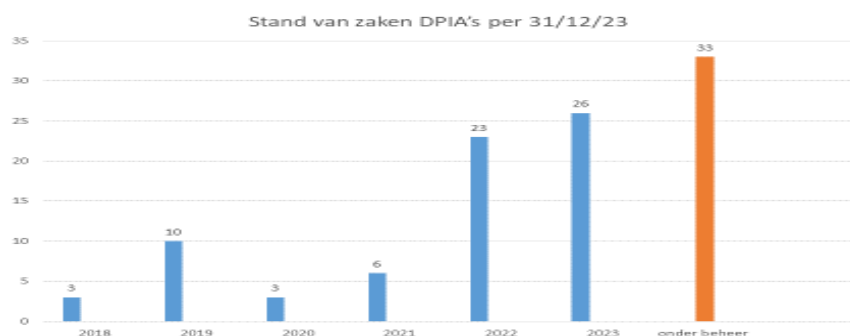
3. Bevindingen control op naleving DPIA's

De uitvraag over naleving betreft alle DPIA's die vanaf zomer 2022 tot peildatum 15 oktober 2023 zijn gemaakt. Gevraagd wordt naar naleving van de afspraken gemaakt in een DPIA (privacy scan) én in het oordeel over de DPIA. Dit betreft in 2023 31 DPIA's. Alle DPIA's die ná 15 oktober 2023 zijn aangeleverd, beoordeeld en vastgesteld zullen in de control cyclus van 2024 meegenomen worden. Onderstaande vragen over de naleving van de DPIA's hebben we uitgevraagd aan de verantwoordelijke concernmanagers.

Naleving van de DPIA's

1. Beschrijf op welke wijze er uitvoering is gegeven aan de genoemde maatregelen (en de implementatie hiervan) zoals benoemd in de bijgevoegde DPIA? Heeft U daarmee volledig voldaan aan de eisen die in de DPIA zijn opgenomen? M.a.w. heeft volledige naleving plaatsgevonden?
2. Op welke wijze heeft *mitigatie* (= verzachting / vermindering) van de genoemde risico's plaatsgevonden? Welke resultaten zijn hierin behaald? Welke problemen ben je tegengekomen? Wat is niet gelukt? Waarom niet?
3. Check Specifieke afspraken zoals verwoord in de DPIA of het oordeel hierover.

DPIA = Data Protection Impact Assessment: een instrument om vooraf de privacy-risico's van een gegevensverwerking in kaart te brengen.



In deze beschouwing zullen we niet nader op de inhoud ingaan, maar met name aangeven óf en zo ja op welke wijze inhoud is gegeven aan naleving van de afspraken. De inhoudelijke feedback en afstemming hierover vindt per dossier met de betreffende afdeling plaats.

De kwaliteit van de beschrijving van de naleving is in 2023 enorm verbeterd. Meerdere afdelingen geven uitgebreid en inhoudelijk toelichting hierover. Dat is een goede stap voorwaarts!

Stoplichten Naleving DPIA's afgegeven tussen mei 2018 – medio oktober 2023

Gesorteerd per afdeling. Aanvullende informatie in bijlage 1.

Naam DPIA	Afdeling	Naleving
Afgerond medio 2022 – 15 oktober 2023		
Gemeentebelastingen (incl. Applicatie Gouw)	FA	●
Bezwaren bij Belastingen No Cure No Pay	FA	●

Naam DPIA	Afdeling	Naleving
Nieuw Financieel Systeem (proces financiën)	FA	●
Leefgeldregeling Oekraïners	IZL	●
Gegevens uitwisseling Inlichtingenbureau en WMO/Jeugdwet	IZL	●
Jongeren in beeld	IZL	n.v.t. project gestopt
Leerplicht (Excl. Wpg werkzaamheden)	IZL	●
Leerplicht Wpg activiteiten	IZL	●
Schuldenknooppunt	IZL	●
GWS / Suite Sociaal Domein	IZL	●
Monitor Sociaal Domein Vernieuwde versie	MO	●
WVGZ (Wet Verplichte Geestelijke Gezondheidszorg)	MO	●
CTR8 Regio- en Gemeentemonitor (Initi8)	MO	●
Gegevensuitwisseling knooppunt in relatie tot Initi8	MO	●
Cameratoezicht Nood Opvang Winkelsteeg	MO	●
Jongeren perspectief fonds JPF	MO	●
Alarmering BHV-ers	PIF	●
Datawarehouse 2022	PIF	●
Gezichtsvergelijking	PU	●
Digitaal verwerken en afhandelen huisbezoeken	PU	Project eind 2023 gestart
Mijn Nijmegen	PU	●
Klantcontactsysteem voor terugbelverzoeken KCC	PU	●
Gebruik afvalpas luiercontainers	SB	Project start in 2024
Definitieve invoering bodycams	SB	●
Inrichting contactregistratie-systeem (CRS) Stadsbeheer	SB	Project start in 2024
Sensoren Stationsoversteek 'Near-misses train station	SR	●
Gegevensuitwisseling Woninginbraak	VJB	●
Dashboard Woninginbraak	VJ 	●
Software ten behoeve van anonimiseren	5.1.2e 	●
Veiligheidshuis	V 	●
Verhuursysteem Amis / LVP	VSA	●

Naam DPIA	Afdeling	Naleving
Afgerond 2018 – medio 2022 Update		
Controle rechtmatigheid inkoop- en betaalproces	FA	●
WMO Klassiek	IZL	●
Project Doe Je mee?	IZL	●
Financieel Expert in de Wijk	IZL	●
Huishoudboekje	IZL	●
Vroeg signalering	IZL	●
Sociale Recherche (anonieme accounts)	IZL	●
Wet Inburgering	IZL	●
Gegevensuitwisseling Inlichtingenbureau en BNK	IZL	●
Buurteams Volwassenen naar Backoffice (BVGN)	MO	●
Buurteams Jeugd en Gezin	MO	●
Fenomeenanalyse	MO	●
Peutermonitor	MO	●
Exchange Online	PIF	●
Corsa	PIF	●
Camera's Dienstpanden	PIF	●
Stembureau App	PU	●
Publiekszaken anonieme accounts	PU	●
MOR Stadsbeheer	SB	●
Toezicht BOA	SB	●
Parkeervergunningensysteem	SB	●
Regionale Toezicht Centrale	SB	●
Passantensensoren	ST	●
Registratiesysteem Regieteam (Gidso)	V 	●
Veiligheid anonieme accounts		●
Veiligheidsknooppunt	VJB	2023 tijdelijk gestopt
IGP		●
Kaartviewer Jaarwisseling	VJB	●
MOR meldingen Jaarwisseling	VJB	●

4. Bevindingen control op naleving Verwerkersovereenkomsten middels een steekproef van 10 vwo's

Uit de steekproefsgewijze controle op de verwerkersovereenkomsten komen de volgende resultaten op naleving naar voren:

Stoplichten Naleving Verwerkersovereenkomsten steekproeven control 2021, 2022 én 2023

Aanvullende informatie in bijlage 2.

Leverancier / Proces – Systeem	Afdeling	Naleving
Unit 4 / CODA / Beheren financiële administratie	FA	Nieuwe aanbesteding
Negometrix aanbestedingsplatform	FA	●
Trias, subsidie volgsysteem	FA	●
Stichting Forus	IZL	●
Allegro / Schuldhulpverlening	IZL	●
Decos	IZL	●
Meta Object / Registreren Jeugdwerkers	MO	●
Kinop. Innovatie nul 13	MO	●
GGD Gelderland Zuid, Groen, gezond en in beweging	MO	●
Konraad / Verwerken gegevens voor uitvoering BOPZ en Huisverbod	MO	●
RAET / beheren Personeelsinformatiesysteem	PIF	●
IRvN / Uitvoeren ICT Dienstverlening en ICT Taken	PIF	●
Picturae Inrichten digitale archieven	PIF	●
KCM Survey / Klanttevredenheidsonderzoek	PU	●
ICTU Controle adresfouten	PU	●
RNI	PU	●
JCC Vastleggen afspraken Stadswinkel	PU	●
Sigmax (Citypermit) Beheren van parkeervergunningen	SB	●
ZAPcam	SB	●
Dynniq, Verkeersregelinstallaties	SB	●
Nibag Groep (energie reductiemaatregelen)	SR	●
Vivacity Near Misses / Bijna ongelukken	SR	●
Amyvon / Registreren gegevens EZ	ST	●
Numina, Passantentellingen	ST	Beëindigt: Vervalt
Cocoon Software Grafisch Ontwerp	VJB	●
Companen, Regionale woningmarkt Monitor	VJB	●
LVP (Amis) / vastleggen reserveringsaanvragen wijkcentra en gymzalen	VSA	●
Sportservice Noord Holland (inhuur sportmedewerkers)	VSA	●
De Haan IT Kassasystemen	VSA	●

Oordeel over de naleving van de afspraken uit verwerkersovereenkomsten

De resultaten uit deze steekproef zijn bedroevend. Slechts 30% van de respondenten geeft aan een verwerkersovereenkomst na te leven. 30% doet dat deels. En van de anderen hebben we 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 drie jaar uitvraag is dit wel teleurstellend.

Voorgesteld wordt om voor het komende jaar (2024) álle verwerkersovereenkomsten op naleving te bezien. Het is aan het management van de tien afdelingen hiervan werk te maken.

Dit hoeft níet te wachten tot de formele uitvraag in november 2024. Op basis van dit signaal kan er nú reeds mee begonnen worden. Ondersteuning vanuit het team privacy kan indien gewenst geleverd worden.

Alle verwerkersovereenkomsten zijn te vinden op de website van de gemeente Nijmegen. Ze worden immers openbaar gemaakt in het 'Verwerkingsregister'.

<https://www.nijmegen.nl/diensten/privacy/verwerkingsregister/>

5. Naleving privacy protocollen

Onderzoek naar het bestaan van en de werking van privacy-protocollen. Vragen:

1. Werkt Uw afdeling met privacy protocollen. Zo ja welke zijn dit?
2. Indien van toepassing: geef aan per protocol op welke wijze naleving van de afspraken, opgenomen in het protocol, plaatsvindt?

Uit de aangeleverde informatie kan alleen het *bestaan* geverifieerd worden. Dat betekent dat we eigenlijk geen goed inzicht hebben. Dit betekent daarmee óók dat over de *werking* geen oordeel gegeven kan worden. Dit kan pas worden opgepakt in 2024.

Afdelingen hebben nog steeds geen goed beeld van de diverse privacy protocollen die afgesloten zijn. Ik kan nog een garantie geven dat we *alle* privacy protocollen met deze uitvraag in beeld hebben. Hierover bestaat nog enige onzekerheid.

Overzicht Privacy Protocollen (bekend)

Publiekszaken:

- Privacy Protocol Publiekszaken.

VJB:

Veiligheid:

- Meldpunt Ondernijning,
- IGP (Intelligence Gestuurd Werken),
- RIEC's-LIEC,
- Regieteams,
- Zorg- en Veiligheidshuis.

Strategie en Onderzoek:

- Nederlandse Code voor Onderzoek en Statistiek / Handboek AVG en statistisch onderzoek

Communicatie: Instructie inzake verwerken persoonsgegevens bij aanvragen Koninklijke Onderscheidingen.

PIF:

P&O:

- Privacy protocol Study tube.

Geen:

Stadsbeheer, Stadsontwikkeling en Stadsrealisatie.

Vastgoed, Sport en Accommodaties: Er is geen officieel privacy protocol. Wel zijn er op de mail vuistregels gecommuniceerd over hoe om te gaan met persoonsgegevens en het benaderen van huurders van onze wijk- en sportcentra. Deze zullen we omzetten in een A4/document, zodat de vuistregels herkenbaar zijn als privacy protocol.

Mogelijk:

MO:

Casussen. Deze moeten nader onderzocht worden.

IZL en FA: geen inzicht over verkregen.

6. Toepassen tafel van 11

De “tafel van 11” is een instrument voor het beleid en controle op naleving. Dit model is 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. De mate van naleefgedrag van vastgestelde regels en uitgangspunten wordt door een aantal aspecten beïnvloed. Deze aspecten vormen samen de ‘Tafel van Elf’. Naar aanleiding van onze bevindingen komen we tot het onderstaande inzicht over de naleving van de afspraken. Dit inzicht geeft handvatten voor nadere aanpak komend jaar:

Spontane naleving zal beter opgepakt worden als de kennis en kunde van de organisatie op het gebied van de AVG in het algemeen en de DPIA’s en verwerkersovereenkomsten in het bijzonder, verhoogd wordt.

De handhavingsdimensie uitgevoerd middels control in 2021, 2022 én in 2023 doet zijn werking. Mensen zijn aan de slag gegaan na de uitvraag. Als geheel is dit proces beter verlopen dan in 2022 en de kwaliteit van de antwoorden is beduidend beter. Sommige afdelingen (zoals IZL) zijn al in staat geweest informatie voorzien van ‘evidence based’ materiaal aan te leveren. Dat is een duidelijke ‘best practise’.

De resultaten uit het controlplan 2023 geven we weer in onderstaande tabel.

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: afwegen. 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.

Het Verwerkingsregister 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.

Gelet op het stijgende bewustwordingsniveau bemerken wij dat het instrument DPIA meer gebruikt en ingezet wordt om (mogelijke) privacy problematieken vooraf in kaart te brengen. Besloten is om voor alle vernieuwingen op het vlak van het verwerken van persoonsgegevens een DPIA op te stellen. Daarmee willen we álle verwerkingen met een mogelijk (hoog) risico waarin met persoonsgegevens wordt gewerkt, in de komende jaren van een DPIA voorzien. Wij realiseren ons dat dit een grote opgave is, maar hebben inmiddels al een aardige slag geslagen.

7. Conclusies

Op basis van deze derde controle op naleving van de afspraken gemaakt in de DPIA's en bij de toets op naleving van de afspraken beschreven in de verwerkersovereenkomsten, komen we tot de volgende beschouwingen:

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:

- Het traject mijn afdeling AVG-proof kan afgerond worden. Dit wil niet zeggen dat de afdelingen AVG-proof zijn. Wél dat alle afdelingen een scan hebben gemaakt en daarmee inzicht hebben in welke acties nog ondernomen moeten worden. De voorwaarden voor het AVG-proof werken zijn daarmee geschapen. Komende jaren gaan we een beweging maken van opzet, naar bestaan en tenslotte naar werking (conform beheer niveau 3). Met het afronden van het traject is 'opzet' gereedgekomen. Nu volgen nog de stappen 'bestaan' en 'werking'. Hierop zal de toetsing van 2024 zich richten.
- Naleving van de DPIA's gaat al beter dan voorgaande jaren. Evidence based aanleveren (aantoonbaar laten zien dat het werkt zoals afgesproken) is nog geen gemeengoed. IZL heeft hierin goede voorbeelden laten zien. Andere afdelingen zouden hier gebruik van kunnen maken.
- De uitvoering van verwerkersovereenkomsten wordt (nog steeds) onvoldoende getoetst op naleving. Dit is teleurstellend te noemen. In 2024 willen we het gehele register laten checken op naleving.
- Privacy protocollen in de organisatie blijven nog steeds onderbelicht. We krijgen langzaam een beter beeld, maar een algemeen overzicht ontbreekt nog.

Kritische noten

- We zijn niet gewend afspraken te toetsen en daarover verantwoording af te leggen. Vooral bij de naleving van de afspraken gemaakt in verwerkersovereenkomsten komt dit (nog steeds) naar boven.
- Accountability als systeemkenmerk kennen we niet. Dat vinden we niet nodig en voelt vaak als overbodig.
- Evidence based als uitgangspunt hanteren we niet. Voorbeeld vanuit IZL biedt perspectief.
- Het afsluiten van een verwerkersovereenkomst of het opstellen van een DPIA wordt nog teveel als een momentopname gezien en als een eenmalige verplichting in een contract of ontwerpproces.
- Facilitering, aansturing of ondersteuning op het gebied van contractmanagement ontbreekt (nog steeds) binnen de organisatie.

Kansen

- Deze derde controle geeft meer duidelijkheid aan het begrip 'naleving'. In de eerste uitvragen hadden veel collega's geen idee wat ze moesten doen. Bij deze derde uitvraag speelt dat in mindere mate. Sommige afdelingen waren reeds voorbereid, als onderdeel van de reguliere P&C cyclus, en gingen meteen aan de slag.
- Het efficiënt managen van verwerkersovereenkomsten zorgt voor alertheid onder leveranciers. Hierdoor heeft een leverancier minder het gevoel om achterover te kunnen leunen. Dit zorgt voor het stijgen van het 'awareness besef' onder medewerkers en leveranciers wat de informatieveiligheid ten goede komt.

Conclusies over naleving van de AVG

Naleving van de AVG is wettelijk vastgelegd op Europees niveau en 'niet naleving' kan forse boetes opleveren vanuit de Autoriteit Persoonsgegevens (opgelegde boetes bij gemeenten per incident lopen in de tonnen). Ik concludeer de uitvoering van naleving middels de volgende vragen, zoals verwoord in onderstaande tabel.

- Willen we (ic de gemeente Nijmegen) de AVG uitvoeren? *Ja.*
- Hebben we daartoe stappen gezet?
Ja, de generieke implementatie van de AVG en daarnaast per afdeling.
- Heeft het bij iedereen urgentie?
Steeds meer, bij een aantal afdelingen is het in de werkprocessen verankerd (internaliseren). Sommigen hebben een team privacy ingericht. Nog niet alle afdelingen hebben een AVG-DNA ontwikkeld.
- Hebben we voldoende kennis en kunde in huis?
Wisselend, is groeiend, het aantal privacy ambassadeurs is fors gegroeid. Nog niet elk bureau kent er een, terwijl dit wel de afspraak is.
- Zijn we als gemeentelijk organisatie volledig 'in control' op de AVG?
Nee deels, generieke maatregelen zijn geïmplementeerd en maar we kunnen nog niet volledig verantwoorden op afdelingsniveau.
- Voldoet de organisatie van de gemeente Nijmegen hiermee aan de wet?
Nee, op een aantal punten, zoals contractnaleving, verantwoording en sturen op risico's, is het nog niet (volledig) op orde.
- Loopt de gemeente Nijmegen hierdoor risico's (behalve imago ook financiële)? *Ja.*
- Moet er vanuit het GMT een tandje bij qua kennis en kunde, sturing, prioritering en aandacht? *Ja.*

Wat mij opvalt is dat deze conclusies enigszins gelijk zijn aan die van voorgaande jaren (2021 en 2022).

Is de organisatie dan niet verbeterd en zijn er dan geen resultaten geboekt?

Dat is in 2023 zeker wel gebeurd. Veel afdelingen hebben forse stappen voorwaarts gezet, zeker op het niveau mijn afdeling AVG-proof en bij het oppakken van DPIA's. We zijn écht op pad om - in 'stoplicht termen' - van rood, naar geel, naar groen te gaan. Alleen is óók géél nog niet groen....

En om dat te bereiken moet - nog steeds - veel effort geleverd worden.

8. Aanbevelingen tot besluitvorming door GMT

Op basis van deze rapportage willen we (vanuit de rollen PO en FG) de volgende besluiten voorleggen:

1. Acties vervolgen uit voorgaande jaren:
 - Gerichte kennis en kunde organiseren vanuit de eigen werkprocessen in de afdelingen. Het team privacy kan hierin ondersteunen, indien gevraagd. Privacy ambassadeurs kunnen hierin een rol vervullen.
 - Structurele inbedding van contractmanagement (bv ten aanzien van verwerkersovereenkomsten) zowel aan het systeem als personele kant en tevens gericht op naleving.
 - In het controlplan 2024 worden *alle* DPIA's welke zijn vastgesteld, weer aan naleving onderworpen.
 - Bij de naleving wordt de nadruk gelegd op 'evidence based' aanlevering vanuit de eindverantwoordelijke concernmanager (die hierop toeziet). De afdeling IZL heeft hiervoor al een eerste (goede) poging gedaan die als best practise gebruikt kan worden.
 - Naleving richt zich op 'spontane naleving'. Hiervoor aanvaardt de concernmanager een inspanningsverplichting.

Nieuw:

2. In het controlplan 2024 wordt elke afdeling uitgevraagd om *alle* verwerkersovereenkomsten waar zij verantwoordelijk voor zijn, te bezien op naleving.
Deze actie kan al in het eerste semester van 2024 gestart worden.




Bijlagen

Naar aanleiding van onze bevindingen komen we tot het onderstaande inzicht over de naleving van de afspraken. Dit inzicht geeft handvatten voor nadere aanpak komend jaar




1. Stand van zaken mijn afdeling AVG-proof per afdeling

Naar aanleiding van onze bevindingen komen we tot het onderstaande inzicht over de naleving van de afspraken. Dit inzicht geeft handvatten voor nadere aanpak komend jaar.

Stand Mijn afdeling AVG Proof eind 2022

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

Stand Mijn afdeling AVG Proof begin 2024

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

2. Naleving DPIA's

Naar aanleiding van onze bevindingen komen we tot het onderstaande inzicht over de naleving van de afspraken. Dit inzicht geeft handvatten voor nadere aanpak komend jaar.

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

Schematisch overzicht naleving DPIA's

a. DPIA's vastgesteld in de periode zomer 2022 – zomer 2023 (eerste check op naleving)

Naam DPIA	Uitvoering genoemde maatregelen / naleving: ja/ neen? Wijze waarop (kort)	Reactie / voorgestelde actie
Gemeentebelastingen (incl. Applicatie Gouw) FA	Ja. Alle benoemde risico's zijn nagelopen en van acties voorzien	Rapportage is adequaat.
Bezwaren bij Belastingen No Cure No Pay FA	Ja. Alle benoemde risico's zijn nagelopen en van acties voorzien	Rapportage volstaat.
Nieuw Financieel Systeem (proces financiën) FA	Ja, DPIA betreffende het proces wordt als zodanig uitgevoerd.	Financieel systeem wordt in de loop van 2024 operationeel gemaakt.
Leefgeldregeling Oekraïners IZL	Neen, geen informatie ontvangen	In 2024 opnieuw uitvragen
Leerplicht (Excl. Wpg werkzaamheden) IZL	Ja. Aandachtspunten in de DPIA waren met name autorisatie en logging.	Beide zijn inmiddels ingericht.
Leerplicht Wpg activiteiten IZL	Ja. Aandachtspunten in de DPIA waren met name autorisatie en logging. Team Leerrecht heeft beide inmiddels ingericht.	Naar aanleiding van de WPG audits is door de toenmalige auditor en Meta Objects contact geweest over de inrichting van JVS om te kunnen voldoen aan de eisen met betrekking tot de uitvoering van de WPG, de wijze waarop de onderdelen kunnen worden ge-audit.
GWS / Suite Sociaal Domein IZL	Deels. Veel acties zijn wel uitgezet en lopen nog door tot medio 2024	Naleving heeft deels plaatsgevonden: checken van acties. Acties zelf zijn echter nog niet afgerond: uitvraag 2024
Schuldenknooppunt IZL	Ja, actiepunten zijn opgepakt	De check op deze logging krijgt voor het eerst zijn beslag in het tweede kwartaal van 2024 om daarna elk kwartaal terug te komen.
Gegevens uitwisseling Inlichtingenbureau en WMO/Jeugdwet IZL	Deels, op dit moment wordt autorisatie inrichting opnieuw vormgegeven.	Meenemen in 2024.
Jongeren in beeld IZL	N.v.t.	Project is gestopt medio 2023. Nog check op archivering en vernietiging in 2024.
WVGZ (Wet Verplichte Geestelijke Gezondheidszorg). MO	Neen, geen rapportage ontvangen	Opnieuw meenemen in 2024
Monitor Sociaal Domein Vernieuwde versie. MO	Neen, geen rapportage ontvangen	Opnieuw meenemen in 2024
CTR8 Regio- en Gemeentemonitor (Initi8). MO	Neen, geen rapportage ontvangen	Opnieuw meenemen in 2024
Gegevensuitwisseling knooppunt in relatie tot Initi8. MO	Neen, geen rapportage ontvangen	Opnieuw meenemen in 2024

Naam DPIA	Uitvoering genoemde maatregelen / naleving: ja/ neen? Wijze waarop (kort)	Reactie / voorgestelde actie
Cameratoezicht Nood Opvang Winkelsteeg. MO	Neen, geen rapportage ontvangen	Opnieuw meenemen in 2024
Jongeren perspectief fonds JPF MO	Neen, geen rapportage ontvangen	Opnieuw meenemen in 2024
Alarmering BHV-ers PIF	Ja, rapportage ontvangen. Maatregelen worden uitgevoerd.	Geen nadere actie noodzakelijk
Datawarehouse 2022 PIF	Ja, rapportage is ontvangen. College heeft besluit genomen aangaande restrisico's. De maatregelen die voorgesteld zijn worden uitgevoerd. GLO's zijn deels en worden (Q1 2024) opgesteld.	Het bestaande datawarehouse gaat vervangen worden. In het eerste half jaar van 2024 wordt hiervoor een inkoopplan opgesteld. Bij het opstellen van de wensen en eisen worden zowel de aanbevelingen uit de DPIA en het oordeel van de FG meegenomen als ook de aanbevelingen uit het advies van de externe adviescommissie digitale ethiek.
Gezichtsvergelijking PU	Ja. De adviezen die in de DPIA staan worden nageleefd. Al deze adviezen zijn in werkprocessen opgenomen. De gebruikers-overeenkomst en alle vragen rondom de software bespreekt de RvIG met de leverancier Oribi. Dit gaat buiten de gemeente om.	Het risico wordt beperkt om dat de werkwijze in een landelijke instructie is verwerkt.
Mijn Nijmegen PU	Ja. Er is voldaan aan de eisen die in de DPIA zijn opgenomen, o.a. op het gebied van role-based access en de toegangsmogelijkheden tot de applicaties. Er is een Key-user aangesteld die verantwoordelijk is voor de inrichting van de applicatie.	Er zijn meermaals werksessies georganiseerd met de leverancier om de inrichting van de applicatie te optimaliseren.
Digitaal verwerken en afhandelen huisbezoeken PU	Nog geen informatie over (DPIA vastgesteld okt. 2023).	Meenemen in controlplan 2024.
Klantcontactsysteem voor terugbelverzoeken KCC PU	Ja. Vraagstuk van inbouwen extra stap in het proces om te voorkomen dat kaarten langer dan een jaar bewaard blijven in Tribe wordt naar verwachting vóór 15 mei 2024 geïmplementeerd.	Restrisico over toekenning en intrekking autorisaties; de enige key user binnen het KCC werkt er nog steeds.
Definitieve invoering bodycams SB	Deels. Melding is dat gewerkt wordt volgens DPIA. Geen onderbouwing gegeven.	2024: aangegeven hoe dit vormgegeven wordt.
Inrichting contactregistratiesysteem (CRS) Stadsbeheer SB	N.v.t. In 2024 opnieuw uitvragen.	In februari 2024 zal het contractregistratiesysteem Tribe binnen Stadsbeheer in gebruik worden genomen. Er zijn daarmee nog geen ervaringen met de naleving van de DPIA.
Gebruik afvalpas luiercontainers SB	N.v.t. In 2024 opnieuw uitvragen.	In februari 2024 zal het passensysteem t.b.v. de luierinzameling in gebruik worden genomen. Er zijn daarmee nog geen ervaringen met de naleving van de DPIA.
Sensoren Stationoversteek 'Near-misses train station' SR	Ja, met name blurring zorgt ervoor dat er geen herkenbare beelden te zien zijn. In de rapportage wordt gesteld: 'Het feit dat de sensoren niet zijn voorzien van een	Actie: In 2024 moet communicatie meer op de gebruikers gericht zijn.






Naam DPIA	Uitvoering genoemde maatregelen / naleving: ja/ neen? Wijze waarop (kort)	Reactie / voorgestelde actie
	bordje met uitleg kan als omissie in de communicatie worden gezien.'	
Zorg –en Veiligheidshuis VJB	Ja. Bij de implementatie van PGA-X is rekening gehouden met het beperken van een te ruime toegang door geautoriseerde personen. Het aan- en afmelden van autorisaties van ketenpartners gebeurt nog handmatig door de Informatiecoördinatoren. Door implementatie van PGA-X is het bijhouden van een schaduwadministratie overbodig. De schaduwadministratie is verwijderd. Er zijn afspraken gemaakt over het halfjaarlijks opschonen van de mailbox en mappen.	De collega's van het Zorg- en Veiligheidshuis krijgen in 2024 een opfrustraining over de AVG vanuit de landelijke vereniging ZVH's. Het Privacy Protocol wordt actief onder de aandacht gebracht bij nieuwe medewerkers tijdens hun inwerkperiode. Na invoering van PGA-X dient er een update / addendum op deze DPIA te worden gemaakt. Dit wordt in 2024 opgepakt door de manager Zorg- en Veiligheidshuis.
Software ten behoeve van anonimiseren VJB	Ja. Er is nog maar zeer sporadisch gebruik gemaakt van de software. Tweemaal is de software gebruikt voor anonimiseren van stukken n.a.v. een Woo-verzoek.	De controle van het algoritme heeft éénmaal plaatsgevonden.
Gegevensuitwisseling Woninginbraak VJB	Ja. De datalevering gebeurt vanuit politiezijde geautomatiseerd, waardoor er weinig handmatig werk aan verbonden is en de kans op fouten geminimaliseerd wordt. De mailbox Data Uitwisseling wordt permanent geleegd zodra de databestanden zijn geïmporteerd. Dit is in 2023 gebeurd.	De mailbox Data Uitwisseling is enkel toegankelijk voor medewerkers met de juiste autorisatie. Deze autorisaties Worden bij personele wisselingen (en ander één keer per jaar) aangepast. In het Convenant Woninginbraken zijn heldere afspraken gemaakt over de aanlevering, opslag, verwerking en verwijdering van gegevens.
Dashboard Woninginbraak VJB	Ja. In het dashboard Woninginbraken wordt per 1 januari 2024 informatie over meldingen vanaf 1 januari 2019 weergegeven. Een gewenste doorontwikkeling is dat het proces van verwijderen van gegevens wordt geautomatiseerd.	Er moet nog een GLO worden opgesteld over de levering van gegevens aan het Data Warehouse. Dit is een actiepunt voor 2024.
Verhuursysteem Amis / LVP VSA	Ja. Naleving is dit jaar getoetst door middel van een accountgesprek in het begin van het jaar, waarin de verwerkersovereenkomst onderwerp op de agenda was.	Er zijn richtlijnen waarnaar gewerkt wordt door LVP. Er zijn uit het accountgesprek geen signalen gekomen over foutief handelen.

b. DPIA's vastgesteld in de periode tot zomer 2023 (tweede of derde check op naleving)

Naam DPIA	Uitvoering genoemde maatregelen / naleving: ja/ neen? Wijze waarop (kort)	Reactie / voorgestelde actie
Controle rechtmatigheid inkoop- en betaalproces (FA)	Ja. Uitvoering is bijna afgerond	2024: Rapportage over project voldoet.
WMO Klassiek (IZL)	Ja, er is getoetst op naleving door een kwaliteitsmedewerker. In 2023 is er een themacontrole uitgevoerd op de dossiers: Complexe en ingrijpende woningaanpassingen.	Prima gedaan. Doorgaan op deze weg!
Project Doe Je mee? (IZL)	Ja, uitgebreide aparte rapportage aangeleverd. Goed voorbeeld van rapportage op naleving (best practise).	2023 én 2024: Steekproeven genomen op de uitvoering. Er wordt stilgestaan bij proportionaliteit en subsidiariteit.
Financieel Expert in de Wijk (FEW) (IZL)	Ja, DPIA wordt nageleefd. DPIA aanvullen met werkproces monitoring. Is nog niet in werking. In 2024 opnieuw uitvragen.	2023: Werkinstructie dataminimalisatie opstellen. Deze is opgesteld en wordt in de algemene werkinstructie opgenomen. De genoemde punten (1t/m 4) zijn in de rapportage opgenomen.
Sociale Recherche anonieme accounts (IZL)	Ja. Er is zelf een controle gedaan op de uitvoering van de DPIA (beslisboom).	2024: Uit de controle valt te concluderen dat controle van social media door de Sociale Recherche eerder uitzondering is dan standaard werkwijze.
Wet Inburgering (IZL)	Er wordt grotendeels gewekt volgens de DPIA. Diverse problematieken (vanuit externe) spelen op dit dossier. Hierop wordt adequaat ingespeeld en naar gehandeld. FG wordt op de hoogte gehouden van problematiek.	2024: Er dienen nog drie bijlagen toegevoegd te worden aan dossier DPIA. Dit betreft de aanbieders van de MAP (Module Arbeid en Participatie), de PVT (het participatieverklaringstraject) en de maatschappelijke begeleiding.
Gegevensuitwisseling Inlichtingenbureau en BNK IZL	Ja, autorisatie en logging zijn opgepakt.	2024: uit toets geen bijzonderheden gekomen.
Huishoudboekje IZL	2021: Ten dele. Alle aanbevelingen zijn opgepakt, maar nog niet volledig tot uitvoering gekomen. Overeenkomst met verwerker moet nog getekend worden (financiën). Pilot ontwikkeling rollen staat geagendeerd voor 2022 (informatie). 2022: Volledige naleving	2021: Intentie vanuit de verantwoordelijke is er zeker. Afhankelijk van bijdragen derden (financiën en Informatie). 2022: Overeenkomst is getekend. Naleving vindt plaats en hierop wordt getoetst. 2023: project 12/06/23 gestopt.
Vroeg signalering IZL	Ja. Rapportage geeft stand van project weer.	2023: processen zijn meer gestroomlijnd. Aantal partners is toe genomen. 2023: actie: addendum op DPIA maken.
Monitor Sociaal Domein IZL	Ja, grotendeels. Probleem zit in het datawarehouse deel load 1. Zie DPIA-datawarehouse. De monitor Sociaal Domein betreft met name Load 2, die volgt op Load 1. Vanuit Load 2 zijn alle privacyaspecten goed ingevuld conform DPIA. Rapportage zie Monitor Sociaal Domein 2022.	2021: In navolging van deze uitvraag is er een gesprek geweest met verantwoordelijken van de monitor. Die was goed en verhelderend. Ter plekke zijn wat adviezen gegeven en aanpassinkjes voorgesteld om de monitor nog meer AVG proof te maken. Afgesproken is vaker af te stemmen. 2022: Update DPIA

Naam DPIA	Uitvoering genoemde maatregelen / naleving: ja/ neen? Wijze waarop (kort)	Reactie / voorgestelde actie
Buurteams Volwassenen naar Backoffice (BVG) (MO)	Geen rapportage ontvangen	Meenemen in 2024
Buurteams Jeugd en Gezin (st. Oidos) (MO)	Geen rapportage ontvangen	Meenemen in 2024
Fenomeenanalyse (MO)	Geen rapportage ontvangen	Meenemen in 2024
Peutermonitor MO	Impliciet, afspraken lijken opgevolgd te worden. Expliciete toets op naleving wordt zo spoedig mogelijk opgepakt. Actie: meenemen in control 2022.	2021: Vraag betekende een 'wake up call': Snelle navraag leerde dat de meeste acties conform DPIA verlopen. Toets is uitgezet. Resultaten volgen. 2022: Wordt opgepakt Q2 2023. 2023: geen rapportage ontvangen.
Camera's dienstpanden PIF	Ja, er is opvolging gegeven aan de aanbevelingen en afspraken.	2021: Afspraken worden opgevolgd. 2022: geen veranderingen. 2023: geen veranderingen.
Corsa PIF	Neen. Project loopt. Vertraagd door capaciteitsproblemen. Voorstel: meenemen in control 2022. 2023: geen nadere info.	2021: Corsa is (nog) niet AVG-proof. 2022: project loopt. Acties uit DPIA worden opgepakt; ingreep in autorisaties; project nog niet afgerond; 2023: Corsa nog niet volledig AVG-proof.
Exchange Online PIF	Ja, belangrijkste maatregel is overigens de scheiding van de Microsoft tenant. Dat wordt voor Nijmegen in 2024 gerealiseerd. Daarmee komen ook enkele nog openstaande maatregelen weer in zicht.	2021: Nog geen antwoord. Onderwerp staat op tactisch overleg met IRvN op 15/12. 2022: actie niet uitgevoerd; opnieuw uitgevraagd. Resultaten meenemen in uitvraag 2023. 2023: Mede n.a.v. deze uitvraag en komst MS365 is afstemming gewenst. Actie: afspraak Q1 2024.
Datawarehouse PIF	Ja. 2023: zie rapportage DPIA Datawarehouse 2022.	2021: De DPIA wordt opnieuw tegen het licht gehouden en geschetste dilemma's worden van een uitkomst voorzien. Discussie wordt gevoerd in stuurgroep AVG jan 2022. 2022: er is een nieuwe DPIA opgesteld. Hierin zijn de aanbevelingen uit de eerdere DPIA grotendeels opgenomen en uitgevoerd. Collegevoorstel wordt in 2023 aangeboden. Actie voor 2023: volgen vorderingen.
Publiekszaken anonieme accounts PU	Er wordt uitsluitend gebruik gemaakt van een algemeen anoniem account. Protocol wordt opgevolgd. Medewerkers werken volgens vier ogen principe	2023: Uitgevoerd en nageleefd.
Stembureau App PU	Ja, naleving heeft plaatsgevonden	2021: Geresulteerd in afspraken in overeenkomsten. 2022: aanbevelingen uit DPIA worden uitgevoerd.
a. IRMA app b. IRMA bellen proef PU	Onduidelijke status. Proef is gestopt, vervolg niet vormgegeven. Advies: besluit over doorgaan of niet. Bij doorgaan nieuwe DPIA opstellen.	2021: Onduidelijkheid over toekomst IRMA-traject. Ook onduidelijkheid wie eigenaar is van dit traject. 2022: traject is gestopt. DPIA KCC is aangeleverd aan FG.

Naam DPIA	Uitvoering genoemde maatregelen / naleving: ja/ neen? Wijze waarop (kort)	Reactie / voorgestelde actie
Regionale Toezicht Centrale (SB)	Wordt uitgevoerd cf. DPIA.	Korte omschrijving (dát) ; geen verdere informatie (hoe?)
MOR Stadsbeheer SB	Ja, op basis van de oorspronkelijke DPIA zijn twee nieuwe DPIA's gemaakt.	2021: Op- en aanmerkingen en aanbevelingen zijn meegenomen in de nieuwe DPIA's. 2022: DPIA wordt gevolgd. Eerste vernietiging cf. DPIA heeft plaatsgevonden. 2023: in Q3 gegevens uit 2017 verwijderd.
Toezicht Algemeen SB	Ja, DPIA specifiek voor niet-BOA's.	2023: Het initiële dashboard Toezicht Algemeen is sinds 2020 niet langer gebruikt. Het dashboard is volledig geïntegreerd in het MOR-dasboard Stadsbeheer. Het dashboard is daarmee vervallen. De DPIA kan daarmee ook komen te vervallen.
Toezicht BOA SB	Ja, DPIA specifiek voor BOA's en wet Wpg.	2021: Uitwerking van adviezen eerdere DPIA. 2022: Dashboard wordt beperkt gebruikt. 2023: vernietiging van gegevens van voor 2017 dient uitgevoerd te worden.
Bodycams eerste en tweede pilot SB	Invoering bodycams definitief. Nieuwe DPIA vastgesteld in 2023. Zie aldaar.	2021: Mede door Corona is de pilot niet volledig uitgevoerd. Er komt een tweede pilot, die wordt meegenomen in 2022. 2022: Bodycams worden definitief.
Parkeervergunningen-systeem SB	Deels, naleving vindt plaats.	2021: De aanbevelingen uit de DPIA worden uitgevoerd. Er is regelmatig contact met de verwerker over de werking van het systeem en de AVG-aspecten daarvan. 2022: Aanpassingen DPIA op onderdelen en update verwerkingsovereenkomst gewenst. 2023: Gelet op een aantal onduidelijkheden dient de DPIA opnieuw onder de aandacht te worden gebracht.
Passantensensoren ST	Ja, impliciet. Geen expliciete check op naleving gedaan. Wel uitvoering gegeven aan de afspraken. Geen reactie gehad op niet naleving.	2021: Impliciete naleving. Dat wil zeggen dat waarschijnlijk gehandeld is conform DPIA, maar niet gecheckt. Kliksysteem geeft geen meldingen en vandaaruit de idee dat er conform gehandeld is. 2022: geen nieuwe informatie ontvangen.
Registratiesysteem Regieteams (Gidso) VJB	DPIA uit 2019 geactualiseerd in 2022.	Zie DPIA uit 2022. Deze komt te vervallen.
Registratiesysteem Regieteams (Gidso) (VJB)	Ja. DPIA uit 2022. 2023: Maatregelen zijn uitgevoerd. In Gidso worden er minder uitgebreide gegevens geregistreerd dan in het oude registratie systeem VIS2.	De naleving van de werkprocessen en werkinstructies van de Regieteams is regelmatig onderwerp in het team overleggen en heidagen met de procesregisseurs Regieteams en de structurele overleggen met de managers van de convenantpartners Regieteams. Door de zeer complexe doelgroep/casuïstiek van de Regieteams is het ook nodig om hierin te blijven bijsturen

Naam DPIA	Uitvoering genoemde maatregelen / naleving: ja/ neen? Wijze waarop (kort)	Reactie / voorgestelde actie
Veiligheid anonieme accounts (V )	Er wordt middels het protocol gewerkt. Geen sock puppets, wel persoonlijke anonieme accounts.	2022: Naleving geschiedt zo goed mogelijk. Alleen logging moet nog geïmplementeerd worden. 2023: Er zijn vanuit de persoonlijke anonieme accounts in 2023 geen vriendschaps- of toegangsverzoeken gestuurd. Personen/groepen worden daarmee niet structureel gevolgd. Het ontbreekt tot op heden aan logging.
Veiligheidsinformatie-knooppunt (VIK) 	2021: Nog niet te duiden: VIK is nog in ontwikkeling. Voorstel: meenemen in control 2022. 2022: werkt grotendeels volgens DPIA	2021: Uitgangspunten DPIA vormen uitgangspunt voor verdere ontwikkeling van het VIK. 2022: VIK zit nog in pilot fase. Er is grotendeels gewerkt volgens DPIA. In 2023 volgt advies voor vervolg: logging moet hierin meegenomen worden. 2023: Naar aanleiding van evaluatie is besloten om het VIK (tijdelijk) in de ijskast te zetten, omdat een aantal technische vereisten nog niet mogelijk waren.
IGP 	Er wordt uitvoering gegeven conform DPIA. Er vindt geen opslag van persoonsgegevens plaats van en via het Nijmeegse domein.	2021: Voorgesteld wordt om een bijeenkomst bij te wonen in 2022 ter toetsing. 2022: conform werkwijze. 2023: conform werkwijze.
Kaartviewer Jaarwisseling 	Ja, er is opvolging gegeven aan de aanbevelingen en afspraken.	2021: Ja, er zijn een puntjes van aandacht, die nu handmatig opgepakt worden. 2022: er wordt grotendeels gewerkt volgens de DPIA. Een verbeterpunt betreft de handmatige acties die nog moeten plaatsvinden. 2023: In 2023 is de kaartviewer niet opengesteld, omdat daar weinig belangstelling voor was.
MOR Meldingen Jaarwisseling 	Ja, er is opvolging gegeven aan de aanbevelingen en afspraken.	2021: Ja, er zijn puntjes van aandacht, die nu handmatig opgepakt worden. 2022: Er wordt grotendeels gewerkt volgens DPIA. Handmatig verwijderen is nog steeds een punt van aandacht. 2023: conform DPIA gehandeld.

* DPIA's die niet meer van toepassing zijn (nieuwe versie; project gestopt, proces anders ingericht) worden in de toetsing niet meer meegenomen. Indien hiervan in 2023 melding wordt gemaakt (zie rapportage boven) vervalt naleving in 2024.

3. Naleving Verwerkersovereenkomsten


Naar aanleiding van onze bevindingen komen we tot het onderstaande inzicht over de naleving van de afspraken. Dit inzicht geeft handvatten voor nadere aanpak komend jaar.

a. Naleving verwerkersovereenkomsten steekproef controlplan 2023

Afdeling / Concernmanager / Leverancier / Proces – Systeem	Naleving en of contractmanagement	Waardoor of hoe vindt naleving plaats?	Reactie / Voorgestelde actie
Trias, subsidie volgsysteem FA	Ja, er is een rapportage door de verwerker opgesteld over de afspraken uit de overeenkomst.	Ja	Akkoord, geen bijzonderheden
Decos IZL	Ja, indirect: TPM Suwinet voor Decos over 2023 waarin wordt voldaan aan het ENSIA-normenkader. Hiermee wordt naleving van de verwerkersovereenkomst feitelijk vastgesteld.	Ja	Akkoord, er loopt nog een navraag over melding van datalekken (wel of geen gemeld).
GGD Gelderland Zuid Groen, gezond en in beweging MO	Neen, geen rapportage ontvangen	Niet	Opnieuw uitvragen 2024.
Picturae Inrichten digitale Archieven PIF	Nee. Er vindt wel periodiek een overleg plaats met de leverancier, maar dit overleg is niet specifiek gericht op nakoming van de verwerkersovereenkomst maar op de algehele dienstverlening	Niet	In de 1e helft van 2024 wordt een overleg ingepland met de leverancier over nakoming van de verwerkersovereenkomst. Dit zal vervolgens jaarlijks herhaald worden.
JCC Vastleggen afspraken Stadswinkel PU	De afdeling Publiekszaken heeft de verwerkersovereenkomst overgedragen gekregen van IZL. Hier moet nog actie worden ondernomen om een compleet beeld te krijgen	Niet	2024: Rapportage volgend jaar.
Dynniq Verkeersregelinstallaties SB	Nee. Onjuiste tenaamstelling bij Dynniq-verkeersregelinstallaties	Niet	Aanpassen tenaamstelling; naleving onderdeel van uitvraag 2024.
Vivacity Near Misses / Bijna-ongelukken SR	De verwerkingsovereenkomst is inmiddels ondertekend.	N.v.t.	Ondertekening is net afgerond. Naleving DPIA heeft wél plaatsgevonden
Numina Passantentellingen ST	De sensoren zijn in de loop van 2022 buiten gebruik gesteld. Het contract met leverancier Intemo is per 1-1-2023 niet meer verlengd.	N.v.t.	Aangezien het contract beëindigd is, is ook de verwerkersovereenkomst vervallen.
Companen Regionale woningmarkt Monitor VJB	VwO met Companen is van feb 2023. Wederzijds ondertekend. Het betreft een jaarlijkse opvraag.	Niet	In Q 1 2024 vindt navraag plaats over de omgang met de gegevens van één jaar eerder.
De Haan IT Kassasystemen VSA	Verantwoordelijk positie is vacant	Niet	Meenemen in 2024.

b. Naleving verwerkersovereenkomsten steekproef controlplan 2021-2022

Leverancier / Proces – Systeem / Afdeling	Naleving en of contractmanagement	Waardoor of hoe vindt naleving plaats?	Reactie / Voorgestelde actie
Unit 4 / CODA / Beheren financiële Administratie FA	Neen, nog geen naleving. Bestaan van VWO was bij uitvoering onbekend 2023: implementatie nieuw financieel systeem.	Vervalt in 2024.	2021/ 2022: In 2022 is er een nieuwe aanbesteding geweest van het financieel systeem. DPIA rondom financieel proces is vastgelegd.
Negometrix.B.V. aanbestedingsplatform FA	Ja, Regelmatig contact over uitvoering	Regelmatig overleg	Cf voorstel: verwerkersovereenkomst bespreking bij upgrade versie 3 naar versie 4.
Kred'it B.V. Allegro/ Schuldhelpverlening IZL	Management certificaat meegestuurd. Hierin geeft verwerker aan gehandeld te hebben conform ISO-normering.	Waarschijnlijk: er is geen relatie zichtbaar tussen certificaat en overeenkomst.	Relatie leggen tussen certificaat en afspraken verwerkersovereenkomst. Daardoor is oordeel lastig te geven.
Stichting Forus / Beheren Meedoen Regeling Stadspas IZL	Ja, naleving heeft plaatsgevonden. Verwerkersovereenkomst is op uitvoering getoetst. Hierbij zijn geen onoverkomelijkheden geconstateerd.	Onderdeel van de ENSIA beoordeling.	2021: Overlap met ENSIA vermijden 2022: geen info ontvangen 2023: onderdeel ENSIA.
Meta Object BV / Registreren van Jeugdzorgwerkers. MO	Geen rapportage ontvangen	Niet	2021: Meenemen in control 2022. 2022 en 2023: geen info verkregen
Innovatie nul13. Kinop MO	Geen rapportage ontvangen	Niet	2023: geen info
Konraad / Verwerken gegevens voor uitvoering BOPZ en Huisverbod MO	Geen rapportage ontvangen	Niet	2021: Meenemen in control 2022. 2022: Wordt meegenomen bij uitvoering nieuwe DPIA. Verantwoordelijke wordt MO 2023: geen info.
RAET / Beheren PersoneelsInformatie- Systeem PIF	Deels. Kwartaloverleg met leverancier maar niet gericht op de nakoming van de verwerkersovereenkomst. Elk jaar wordt de ISAE 3402 type II opgevraagd. Deze International Standard on Assurance Engagement is een verklaring m.b.t. de IT-security en privacy die wordt opgesteld na een audit die VISMA/RAET laat uitvoeren door een accountant (over 2020 Deloitte).	Niet, komen specifieke vragen naar voren over ondersteuning bij uitvoer contractmanagement.	2021: Meenemen in control 2022. 2022: Jaarlijks wordt de ISAE 3402 type II verklaring opgevraagd. Dit betreft een uitgebreide verklaring over gegevensbescherming en privacy. 2023: geen nadere nieuwe informatie
IRvN / Uitvoeren ICT dienstverlening en ICT Taken PIF	Ja. Er komt een nieuwe generieke verwerkersovereenkomst welke iRvN kan afsluiten met al haar deelnemers. Verwachting is dat deze overeenkomst nog in januari 2024 getekend zal worden	VWO wordt nageleefd. Aantal acties zijn ondernomen.	2023: Uitgevoerde acties: - Meldplicht datalekken en Beveiligingsincidenten - Plan van aanpak incidenten - Inzage logboek - Autorisatiematrix: er is gestart met het opstellen van een autorisatiematrix In 2024 verwachting implementatie.
ICTU. Controle adresfouten BRP PU	Verwerkersovereenkomst 30/09/22 goedgekeurd..	Ja	2023: Jaarlijks meerdere bijeenkomsten tussen afnemers en verwerkers over ontwikkelingen en naleving.

Leverancier / Proces – Systeem / Afdeling	Naleving en of contractmanagement	Waardoor of hoe vindt naleving plaats?	Reactie / Voorgestelde actie
RNI PU	Twee keer per jaar account gesprek over naleving	Vaste afspraak	Naleving vindt plaats
KCM Survey BV / Klanttevredenheids- onderzoek Stadswinkel PU	Neen, geen specifiek of proactief overleg over nakoming verwerkersovereenkomst. 2023: Proces is akkoord en leidt niet tot een DPIA.	Geen controle op sub verwerkers.	2021: Meenemen in control 2022. 2022: geen nieuwe info ontvangen. 2023: actie op sub verwerkers.
Sigmax (Citypermit) / Beheren van het Parkeervergunningen- systeem SB	Deels. Er is halfjaarlijks overleg. Ten tijde van updates is er bijna wekelijks overleg. In de overeenkomsten wordt rekening gehouden met de eisen van de AVG. Bij updates zijn er release notes waarin alle wijzigingen staan genoteerd. Hierbij wordt rekening gehouden met AVG eisen.	Contractmanagement is niet geborgd in een systeem.	2021: Meenemen in control 2022. 2022: contractmanagement nog steeds niet geborgd; Opnieuw toetsen in 2023. 2023: wijzigingen rondom verwerkingsovereenkomsten (ander Hosting-partij bij Sigmax). Actie: Doorvoeren wijzigingen.
Zapcam Nijmegen SB	Pilot is afgerond; verwerkingsovereenkomst betrof pilot	N.v.t.; periode is afgesloten	Nieuwe verwerkersovereenkomst opstellen
Nibag Groep BV. Energie reductiemaatregelen SR	Ja, Korte rapportage op basis van navraag. Contact met Nibag is er wekelijks. Dat gaat primair over uitvoering van projecten. Hierbij wordt ook ingezoomd op de naleving van afspraken.	Ja, grotendeels	Na afmelden van woningen (eind saneringsproject) worden de persoonlijke gegevens uit dossier verwijderd. Voor de gemeente Nijmegen doet Nibag meerdere projecten, maar geen van deze projecten is zo ver.
Amyyon / Registreren gegevens relaties EZ ST	Ja, grotendeels. Er is regelmatig contact geweest bij de inrichting, waarbij de uitgangspunten van de AVG meegenomen zijn. 2023: Er vindt geregeld overleg plaats met de leverancier.	Er is (nog) geen systematische periodieke controle uitgevoerd.	2021: Meenemen in Control 2022 2022: geen nieuwe informatie 2023: De naleving van de verwerkersovereenkomst is tot dusverre niet getoetst.
Cocoon Software Technology B.V. Grafische ontwerp.  B	Incidenteel accountgesprekken met Cocoon over ontwikkelingen en als er bijvoorbeeld nieuwe functionaliteiten zijn.	Deels	In 2024 is er een nieuw accountgesprek staan. Meenemen in controlplan 2024.
Compudienst LVP (Amis) Vastleggen Reserverings- Aanvragen wijkcentra en Gymzalen. VSA	Ja, Naleving is dit jaar getoetst door middel van een accountgesprek in het begin van het jaar, waarin de verwerkers-overeenkomst op de agenda stond.	Er zijn richtlijnen waarnaar gewerkt wordt door LVP.	2021: Meenemen in control 2022. 2022: DPIA over het verhuurproces. 2023: Uit het accountgesprek geen signalen over foutief handelen.
Sportservice Noord- Holland. VSA	Dit was nog niet onder de aandacht. Deze moet nog opgesteld worden. Volgt in 2024.	Niet	Meenemen in 2024.

PK/19/03/2024/v.1.0

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	6, 7, 21, 24