

Interne audit 2022/2023 Wet politiegegevens

1 november 2022 tot en met 31 oktober 2023

Gemeente Nijmegen

Datum:	30 november 2023
Rapportnummer:	2C-2023-556
Versie:	1.0
Status:	Definitief

Versiebeheer

Versie	Datum	Status	Naam
0.1	28 november 2023	Initiële versie	2-Control B.V.
1.0	30 november 2023	Definitief	2-Control B.V.

Inhoud

1	Algemeen	5
1.1	Achtergrond en doelstelling	5
1.2	Scope	5
1.3	Auditplanning	5
1.4	Aanpak	6
1.5	Verspreiding en gebruik	7
1.6	Bevindingen	7
2	Normenkader	9
3	Bevindingen en aanbevelingen	15
3.1	Algemene bevindingen en aanbevelingen	15
3.2	Detailbevindingen en aanbevelingen	16
3.3	Detailbevindingen en aanbevelingen technische en organisatorische maatregelen	33

Management samenvatting

Op 22 september en 14 november 2023 heeft 2-Control de interne Wpg audit over de periode 31 oktober 2022 tot 1 november uitgevoerd (hierna genoemd "auditperiode"). Zoals in de auditplanning in het vorige interne auditrapport staat beschreven is ervoor gekozen om niet elk jaar het volledige normenkader te toetsen, maar om jaarlijks een deel te toetsen, zodanig dat in 4 jaar het volledige normenkader wordt getoetst over alle verwerkingen. Voor deze auditperiode is gekozen om Domein I (Toezicht en Handhaving) in scope op te nemen:

Audit jaar	Te toetsen normen en scope
2022 / 2023	<ul style="list-style-type: none"> • Toezicht en Handhaving (Openbare Ruimte) • GISC CityControl (TPM) • GISC Brickyard (TPM – nog niet beschikbaar) • GISC Blackberry Messenger (SOC2) • GISC ICT (ter ondersteuning van netwerkschijven en Corsa)

De scope van de uitgevoerde interne audit bij Gemeente Nijmegen bestond uit de hierna genoemde verwerkingen van politiegegevens:

#	Organisatieonderdeel	Domein	Processen/verwerkingen	Applicaties
1	Toezicht & Handhaving (Openbare Ruimte)	I	Opsporing strafbare feiten in domein I (openbare ruimte)	CityControl Brickyard Blackberry Messenger Corsa Netwerkschijven

Bevindingen

Van de 17 getoetste normen is bij de meeste normen een verbetering te zien ten opzichte van de initiële audit in 2021 en hercontrole begin 2023. 7 normen voldoen volledig aan opzet en bestaan en voor 2 van deze 7 normen was vast te stellen dat gedurende de hele auditperiode aantoonbaar aan de norm werd voldaan (werking). Dit is mede het gevolg dat in de 2^e helft van de auditperiode meerdere herstelacties zijn uitgevoerd waardoor meerdere maatregelen niet de gehele auditperiode hebben gewerkt. Voor de overige 10 normen is vastgesteld dat deze inmiddels wel in opzet (deels) voldoen, maar in bestaan nog niet (volledig) konden worden vastgesteld. Dit was enerzijds het gevolg dat beschreven maatregelen nog niet daadwerkelijk waren geïmplementeerd of dat externe partijen niet (aantoonbaar) voldeden aan de normvereisten

Van de zogenaamde General IT Controls (basisbeveiliging) is met name gericht op het IT-beheer van IRvN betreffende de beveiliging van Wpg gegevens op netwerkschijven en in Corsa. Daarnaast hebben we externe audit-verklaringen (TPM / SOC2) opgevraagd bij de externe dienstverleners die een online applicatie aanbieden waarin Wpg gegevens worden verwerkt. Dit is in opzet en bestaan deels voldoende aangetoond waardoor de conclusies gelijk zijn aan de hercontrole begin 2023.

Voor een overzicht van bevindingen verwijzen wij naar paragraaf 1.6 en voor een detailuitwerking naar hoofdstuk 3.

Aanbevelingen

Vorig jaar is een intern audit rapport opgesteld. De aanbevelingen in dit rapport ten aanzien van Domein I zijn opgevolgd of onder handen. Belangrijk uitgangspunt is een domein specifiek handboek wat inmiddels in concept is opgesteld en waarin handvatten vastliggen om controleerbaar de Wpg-normen na te leven. Wij adviseren dit handboek definitief te maken, de implementatie af te ronden en de naleving te borgen.

De aanbevelingen zijn verder uitgewerkt in hoofdstuk 3.

1 Algemeen

1.1 Achtergrond en doelstelling

Alle organisaties met boa's in dienst moeten, voor verwerkingen in het kader van opsporing, voldoen aan de Wet Politiegegevens en het Besluit Politiegegevens. Onderdeel van deze wet is het vierjaarlijks uitvoeren van een externe privacy audit en het jaarlijks uitvoeren van een interne audit.

De jaarlijkse interne audit heeft tot doel op systematische wijze toetsen of voor één, dan wel een aantal onderdelen van de wet op adequate wijze uitvoering is gegeven aan de bepalingen van de wet. Hiervoor heeft een beoordeling plaatsgevonden van de opzet, bestaan en de werking van maatregelen en procedures die in naleving van de wettelijke eisen moeten voorzien.

Dit rapport is het resultaat van de uitgevoerde interne audit bij Gemeente Nijmegen over de periode 1 november 2022 tot en met 31 oktober 2023.

Een opdracht tot het uitvoeren van een interne audit is geen controle-, beoordelings- of andere assurance-opdracht. Een opdracht tot het uitvoeren van een interne audit omvat niet het door de interne auditor verkrijgen van informatie met als doel, in welke vorm dan ook, een oordeel te geven of een assurance-conclusie te trekken. Het doel van het interne audit rapport is om de organisatie inzicht te verschaffen in of de organisatie op adequate wijze uitvoering heeft gegeven aan de bepalingen van de wet en op basis daarvan verbeteracties uit te voeren.

1.2 Scope

De scope van de uitgevoerde interne audit bij Gemeente Nijmegen bestond uit de hierna genoemde verwerkingen van politiegegevens:

#	Organisatieonderdeel	Domein	Processen/verwerkingen	Applicaties
1	Toezicht & Handhaving (Openbare Ruimte)	I	Opsporing strafbare feiten in domein I (openbare ruimte)	CityControl Brickyard Blackberry Messenger Corsa Netwerkschijven

Tijdens de interne audit is geen onderzoek uitgevoerd naar hierboven niet genoemde verwerkingen van politiegegevens.

1.3 Auditplanning

Conform de wet dient jaarlijks voor één, dan wel een aantal onderdelen van de wet systematisch te worden getoetst of op adequate wijze uitvoering is gegeven aan de bepalingen van de wet. Bij Gemeente Nijmegen zijn voor 2022/2023 de volgende normen getoetst:

Audit jaar	Te toetsen normen en scope
2022 / 2023	<ul style="list-style-type: none"> • Toezicht en Handhaving (Openbare Ruimte) • GISC CityControl (TPM) • GISC Brickyard (TPM – nog niet beschikbaar) • GISC Blackberry Messenger (SOC2) • GISC ICT (ter ondersteuning van netwerkschijven en Corsa)

Dit is onderdeel van onderstaande totaalplanning:

Jaar	Onderdeel
2022	Domein V
2023	Domein I

Jaar	Onderdeel
2024	Domein III
2025	Overkoepelende normen

1.4 Aanpak

Wij hebben voor het uitvoeren van de interne audit de volgende activiteiten uitgevoerd:

1. Bestuderen documentatie;
2. Interviewen van onderstaande personen:
3. Waarnemingen in systemen.

Datum	Domein	Interviewee	Functie
22-9 & 14-11	Domein 1	5.1.2e	Interim Manager T&H
22-9 & 14-11	Overkoepelen	5.1.2e	Privacy officer
22-9 & 14-11	Domein 1	5.1.2e	Operationeel Leidinggevende T&H
22-9 & 14-11	Domein 1	5.1.2e	Bureau Parkeren (functioneel beheer)
22-9 & 14-11	Domein 1	5.1.2e	Business Adviseur I&A (Stadsbeheer)
22-9 & 14-11	Overkoepelend	5.1.2e	CISO
22-9	IRvN	5.1.2e	Teamleider IRvN
22-9 & 14-11	IRvN	5.1.2e	Functioneel beheerder Corsa
22-9	Overkoepelend	5.1.2e	Informatieadviseur
14-11	Domein 1	5.1.2e	Juridisch medewerker
14-11	Domein 1	5.1.2e	Tactisch Handhaver
14-11	Domein 1	5.1.2e	Coördinator Afdeling Parkeren
14-11	Overkoepelend	5.1.2e	FG
14-11	Overkoepelend	5.1.2e	IBD (t.b.v. Corsa)
14-11	Domein 1	5.1.2e	Specialist RTC en Parkeren

De interne auditor maakt bij het uitvoeren van deze activiteiten gebruik van de volgende criteria.

Opzet	De organisatie heeft de beheersingsmaatregelen beschreven die voorzien in de borging van de wettelijke eisen met betrekking tot de verwerking van politiegegevens door boa's.
Bestaan	De organisatie heeft de beheersingsmaatregelen overeenkomstig de opzet daadwerkelijk geïmplementeerd en toegepast.
Werking	De organisatie heeft de beheersingsmaatregelen gedurende de verslaggevingsperiode volgens de opzet toegepast, ingeval van handmatige beheersingsmaatregelen zijn deze toegepast door competente en bevoegde personen.

1.5 Verspreiding en gebruik

Dit rapport is vertrouwelijk, alleen bestemd voor intern gebruik en mag niet worden verspreid naar derden partijen zonder uitdrukkelijke toestemming. Dit rapport kan worden gebruikt om intern te rapporteren aan het verantwoordelijk management.

1.6 Bevindingen

Wij hebben vastgesteld dat de hiernavolgende Wpg onderwerpen niet (rood) of niet volledig (oranje) zijn opgezet, bestaan en/of effectief werken. Zoals opgenomen in de beschrijving van de beheersingsdoelstellingen, beheersmaatregelen en de bevindingen en aanbevelingen waren deze interne beheersmaatregelen niet gedurende de gehele verslagperiode in afdoende mate opgezet, hebben niet bestaan en/of werkten niet effectief.

Voor de volledigheid zijn de onderwerpen die afdoende zijn opgezet, geïmplementeerd en effectief werkten ook vermeld (groen). Dit geldt eveneens voor de onderwerpen die niet zijn onderzocht (grijs).

De redenen waarom normen niet zijn onderzocht zijn als volgt aangeduid:

*) Bestaan en/of werking bij betreffende norm niet kunnen toetsen wegens non-occurrence;

**) Norm geheel niet van toepassing omdat het betreffend proces zich niet voordoet bij Gemeente Nijmegen

***) niet onderzocht in het kader van deze interne audit

Omdat binnen Gemeente Nijmegen meerdere verwerkingen van politiegegevens plaatsvinden, waarbij de oordelen per onderwerp onderling afwijken, hebben we de bevindingen per verwerking weergegeven.

Domein I: Opsporing strafbare feiten in domein I (openbare ruimte)

Onderwerpen	Interne audit		
	Opzet	Bestaan	Werking
1. Reikwijdte ***			
2. Doelbinding			
3. Noodzakelijkheid & rechtmatigheid, vermelding herkomst			
4. Juistheid en volledigheid politiegegevens			
5. Onderscheid feiten en persoonlijk oordeel			
6. Gegevensbescherming door beveiliging en ontwerp ***			
7. Gegevensbescherming door standaardinstellingen ***			
8. Gegevensbeschermingseffectbeoordeling / Data protection impact assessment			
9. Bijzondere categorieën van politiegegevens **			
10. Autorisaties en toegang tot politiegegevens			
11. Autorisaties: aanwijzen functionarissen **			
12. Onderscheid tussen verschillende categorieën van betrokkenen **			
13. Verwerker en Verwerkersovereenkomst			
14. Geheimhoudingsplicht			
15. Geautomatiseerde individuele besluitvorming			
16. Uitvoering van de dagelijkse politietaak			
17. Ter beschikking stellen van politiegegevens binnen het Wpg-domein **			
18. Geautomatiseerd vergelijken en in combinatie zoeken **			
19. Ondersteunende taken **			
20. Bewaartermijnen, verwijderen en vernietigen			

Onderwerpen	Interne audit		
	Opzet	Bestaan	Werking
21. Verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee			
22. Doorgiften aan derde landen **			
23. Verstrekking aan derden structureel voor samenwerkingsverbanden			
24. Rechtstreekse verstrekking **			
25. Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering ***			
26. Register			
27. Documentatie			
28. Logging			
29. Audits			
30. Melding datalekken			
31. Functionaris voor gegevensbescherming			

Technische en organisatorische maatregelen	Interne audit		
	Opzet	Bestaan	Werking
01 Wijzigingenbeheer			
02 Logische toegangsbeveiliging			
03 Beheer van kwetsbaarheden (patchmanagement)			
04 Cryptografie			
05 Vulnerability scans en Penetratietesten			

2 Normenkader

Om de privacy van de verwerkte politiegegevens ten behoeve van de wettelijke taak te kunnen waarborgen en te kunnen voldoen aan de eisen die de wet daaraan stelt, heeft Gemeente Nijmegen beheersingsmaatregelen getroffen in lijn met de illustratieve beheersingsmaatregelen uit de NOREA Handreiking Privacy audit Wpg (boa). Die illustratieve beheersingsmaatregelen zijn gebaseerd op de Wet politiegegevens en het Besluit politiegegevens buitengewoon opsporingsambtenaren en omvatten de te verwachten onderwerpen en -beheersingsmaatregelen, gericht op beheersing van privacy in gegevensverwerkende processen en indicatieve controles, in lijn met de geldende wet- en regelgeving.

Onderstaand zijn deze onderwerpen en illustratieve beheersingsmaatregelen weergegeven.

Onderwerpen en beheersingsmaatregelen
<p>1. Reikwijdte De verwerkingsverantwoordelijke heeft bestanden met politiegegevens binnen de organisatie geïdentificeerd en gedocumenteerd.</p>
<p>2. Doelbinding Politiegegevens worden alleen verwerkt als dat nodig is voor de in de wet genoemde doeleinden. Geborgd is dat bij het verwerken van politiegegevens altijd sprake is van doelbinding en dat de gegevens niet op een, met die doeleinden onverenigbare wijze, worden verwerkt.</p>
<p>3. Noodzakelijkheid en rechtmatigheid, vermelding herkomst Er wordt geborgd dat de politiegegevens daartoe toereikend, ter zake dienend en beperkt zijn tot wat noodzakelijk is (niet bovenmatig) en dat de herkomst van gegevens voor art 9 verwerkingen wordt vermeld.</p>
<p>4. Juistheid en volledigheid politiegegevens</p> <ul style="list-style-type: none"> De verwerkingsverantwoordelijke heeft controles op de kwaliteit ingericht ten behoeve van de borging van de juistheid en nauwkeurigheid van politiegegevens. Er zijn procedures opgesteld voor het vernietigen en rectificeren van politiegegevens.
<p>5. Onderscheid feiten en oordeel Er zijn maatregelen genomen om politiegegevens die op feiten zijn gebaseerd, voor zover mogelijk, te onderscheiden van politiegegevens die op een persoonlijk oordeel zijn gebaseerd.</p>
<p>6. Gegevensbescherming door beveiliging en ontwerp</p> <ul style="list-style-type: none"> Er is (aantoonbaar) een risicoanalyse uitgevoerd waaruit het risiconiveau blijkt en identificeert, evalueert en mitigeert systematisch en periodiek factoren die het beschermen van politiegegevens tegen ongeoorloofde of onrechtmatige verwerking en tegen opzettelijk verlies, vernietiging of beschadiging in gevaar brengen en past de maatregelen hierop aan. De organisatie heeft gegevensbeschermingsbeleid en procedures ontwikkeld en vastgesteld. De verwerkingsverantwoordelijke heeft de maatregelen die nodig zijn om het risico te beperken (passende technische en organisatorische maatregelen) aantoonbaar geïmplementeerd. Privacy by design wordt toegepast/geborgd (bijv. bij ontwikkelingen/ wijzigingen). De verwerkingsverantwoordelijke kan aantonen dat de verwerking van politiegegevens wordt verricht in overeenstemming met wat bepaald is in de wet.
<p>7. Gegevensbescherming door standaardinstellingen De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen om te waarborgen dat standaard:</p> <ul style="list-style-type: none"> alleen die politiegegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking; politiegegevens niet zonder tussenkomst van een natuurlijke persoon voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt.

Onderwerpen en beheersingsmaatregelen
<p>8. Gegevensbeschermings-effectbeoordeling / Data protection impact assessment (DPIA)</p> <ul style="list-style-type: none"> • Indien een verwerking waarschijnlijk een hoog risico voor de rechten en vrijheden van personen oplevert worden binnen de organisatie de risico's systematisch geïdentificeerd, beoordeeld en aangepakt door middel van een DPIA die ten minste aan de eisen gesteld in de wet voldoet. • De verwerkingsverantwoordelijke beoordeelt, indien nodig of wanneer sprake is van een verandering van het risico, of de verwerking in overeenstemming met de DPIA wordt uitgevoerd en past de DPIA zo nodig aan.
<p>9. Bijzondere categorieën van politiegegevens</p> <p>Er vindt geen verwerking van bijzondere categorieën van politiegegevens plaats, tenzij:</p> <ul style="list-style-type: none"> • Dat onvermijdelijk is voor het doel van de verwerking. • Dit in aanvulling is op de verwerking van andere politiegegevens betreffende de persoon. • De gegevens afdoende zijn beveiligd.
<p>10. Autorisaties en toegang tot politiegegevens</p> <ul style="list-style-type: none"> • Er is een systeem van autorisaties dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid. Dit houdt in dat: De verwerkingsverantwoordelijke heeft die personen die vanuit hun functie en de wet toegang mogen hebben tot bepaalde politiegegevens geautoriseerd voor alleen die gegevens (need-to-know). • Er is een proces voor het toewijzen, wijzigen en intrekken van autorisaties t.b.v. de toegang tot politiegegevens. • Er zijn maatregelen vastgesteld en geïmplementeerd die de identiteit en de toegangsrechten van een gebruiker controleert en rechtmatige toegang tot de gegevens borgt.
<p>11. Autorisaties: aanwijzen functionarissen</p> <p>Er is een actuele lijst van, door de verwerkingsverantwoordelijke aangewezen, bevoegde functionarissen.</p>
<p>12. Onderscheid tussen verschillende categorieën van betrokkenen</p> <p>De verwerkingsverantwoordelijke heeft geborgd dat, voor zover mogelijk, duidelijk onderscheid wordt gemaakt in de verschillende categorieën van betrokkenen.</p>
<p>13. Verwerker en Verwerkersovereenkomst</p> <ul style="list-style-type: none"> • De verwerker stelt de verwerkingsverantwoordelijke alle informatie ter beschikking die nodig is om aantoonbaar te maken dat de verplichtingen in de Verwerkersovereenkomst en de Wpg worden nageleefd en die nodig is om audits mogelijk te maken. • De verwerking door een verwerker vindt alleen plaats als een verwerkingsverantwoordelijke afdoende garanties heeft over de toereikendheid van de geïmplementeerde technische en organisatorische maatregelen. • Bij elke uitvoering van een gegevensverwerking door een verwerker zijn de taken en afspraken schriftelijk vastgesteld en vastgelegd in een (toereikende) overeenkomst of andere rechtshandeling. • Er zijn afspraken vastgesteld en vastgelegd m.b.t. de handelswijze bij een inbreuk op de beveiliging. • Een andere partij is alleen ingeschakeld bij de uitvoering van de verwerking met toestemming van de verwerkingsverantwoordelijke. Aan deze andere verwerker (subverwerker) is bij een overeenkomst dezelfde verplichtingen inzake gegevensbescherming opgelegd.
<p>14. Geheimhoudingsplicht</p> <p>Er is geborgd dat de ambtenaar van politie of de persoon aan wie politiegegevens ter beschikking zijn gesteld formeel bekend is met de plicht tot geheimhouding en de consequenties bij schending van deze plicht.</p>

Onderwerpen en beheersingsmaatregelen
<p>15. Geautomatiseerde individuele besluitvorming</p> <ul style="list-style-type: none"> Besluiten gebaseerd uitsluitend op geautomatiseerde verwerking dat voor de betrokkene nadelige rechtsgevolgen heeft of hem in aanmerkelijke mate treft, worden niet genomen tenzij voorzien is in de voorwaarden genoemd in de wet. Het verbod op het gebruik van profilering die leidt tot discriminatie van personen op grond van de bijzondere categorieën van politiegegevens (art 5) is bekend binnen de organisatie. Dit beperkte verbod op profilering is onderwerp van de bewustwordingssessies binnen de organisatie.
<p>16. Uitvoering van de dagelijkse politietaak</p> <ul style="list-style-type: none"> Geborgd is dat art 8 politiegegevens één jaar na de datum van de eerste verwerking zodanig worden opgeslagen (achter een schot worden geplaatst) dat ze alleen nog beschikbaar komen voor verdere verwerking op basis van de vergelijking van gegevens (hit-no-hit basis). Geborgd is voor zover dat noodzakelijk is met het oog op de uitvoering van de dagelijkse politietaak politiegegevens ten aanzien waarvan in art 8 lid 1 genoemde termijn is verstreken geautomatiseerd worden vergeleken met politiegegevens die worden verwerkt op grond van art 8 lid 1 teneinde vast te stellen of verbanden bestaan tussen de betreffende gegevens. De gerelateerde gegevens kunnen verder worden verwerkt met het oog op de uitvoering van de dagelijkse politietaak.
<p>17. Ter Beschikking stellen (voor verdere verwerking)</p> <ul style="list-style-type: none"> Geborgd is dat de verdere verwerking van art 9 gegevens alleen plaats vindt na toestemming (aantoonbaar) van de daartoe bevoegde functionaris. Geborgd is dat de ter beschikking stellen van politiegegevens aan bevoegde autoriteiten in andere lidstaten van de Europese Unie of aan organen en instanties belast met de taken, bedoeld in art 1, onderdeel a conform de richtlijnen gesteld in de wet plaatsvindt.
<p>18. Geautomatiseerd vergelijken en in combinatie zoeken</p> <ul style="list-style-type: none"> Geborgd is dat gegevens alleen geautomatiseerd worden vergeleken met andere politiegegevens of met andere dan politiegegevens binnen de richtlijnen gesteld in art 11. Geborgd is dat gegevens alleen in combinatie met elkaar worden verwerkt binnen de richtlijnen gesteld in art 11 lid 4. Geborgd is dat het in combinatie verwerken van art 8 politiegegevens beperkt is tot de ambtenaren van politie die daarvoor geautoriseerd zijn. Geborgd is dat de ambtenaren die geautomatiseerd vergelijken en ambtenaren die in combinatie zoeken over voldoende kennis en vaardigheden beschikken.
<p>19. Ondersteunende taken</p> <p>Geborgd is dat voor de verwerkingen bedoeld in art 13 lid 1 t/m 3, van tevoren is voldaan aan de schriftelijke vereisten (art 13 lid 4).</p>
<p>20. Bewaartermijnen, verwijderen en vernietigen</p> <ul style="list-style-type: none"> Politiegegevens worden niet langer bewaard dan de minimale tijd die nodig is, zoals vereist door de toepasselijke wet- en regelgeving, of voor de doeleinden waarvoor deze zijn verwerkt. De verwerkingsverantwoordelijke voorziet in voldoende waarborgen om te bewerkstelligen dat de gegevens conform de wet worden gecontroleerd, verwijderd en vernietigd. Geborgd is dat Politiegegevens na verwijdering maximaal vijf jaar worden bewaard. Indien van cultureel of historisch belang kan worden afgezien van vernietiging van de gegevens. Er wordt dan aan de bewaareisen zoals genoemd in de Archiefwet voldaan.

Onderwerpen en beheersingsmaatregelen

21. Verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee

- Geborgd is dat politiegegevens alleen worden verstrekt aan personen of instanties buiten het politiedomein, voor zover dit noodzakelijk is voor de doeleinden zoals deze in de Wet politiegegevens en het Besluit politiegegevens zijn genoemd.
- Geborgd is dat wanneer gegevens verstrekt worden er wordt voldaan aan de documentatieplicht (conform 6 lid 4 Bpg).
- Geborgd is dat verstrekking alleen plaatsvindt in overeenstemming met het bevoegd gezag indien dit vereist is in de wet.
- Bij verstrekkingen is geborgd dat de ontvangende partij wordt gewezen op zijn geheimhoudingsplicht.
- De juistheid, volledigheid, actualiteit en betrouwbaarheid van politiegegevens bij verstrekking wordt, voor zover mogelijk, gecontroleerd en inzichtelijk gemaakt voor de ontvangende partij.
- Er is een procedure voor het onverwijld in kennis stellen van de ontvanger van politiegegevens indien geconstateerd wordt dat onjuiste politiegegevens zijn verstrekt of dat politiegegevens op onrechtmatig wijze zijn verstrekt.

22. Doorgiften aan derde landen

- De doorgifte van gegevens aan verwerkingsverantwoordelijke in derde landen vindt alleen plaats indien er een adequaatsheidsbesluit is van de Commissie van de Europese Unie of indien één van de uitzonderingsgronden zoals genoemd in de wet van toepassing is.
- De doorgifte van gegevens aan derde landen wordt vastgelegd (documentatieplicht).
- Indien doorgifte plaatsvindt op basis van art 17a lid 2 onderdeel a of b, lid 3 of lid 5 is (aantoonbaar) voldaan aan de gestelde eisen in de wet.
- Indien politiegegevens van een andere lidstaat afkomstig worden doorgegeven aan derde landen is de toestemming van de verantwoordelijke autoriteit van deze lidstaat beschikbaar.

23. Verstrekking aan derden structureel voor samenwerkingsverbanden

- De verwerkingsverantwoordelijke heeft inzicht in de samenwerkingsverbanden waarbij politiegegevens worden verstrekt.
- In de beslissing voor het verstrekken van politiegegevens t.b.v. een samenwerkingsverband wordt vastgelegd:
 - Ten behoeve van welk zwaarwegend algemeen belang de verstrekking noodzakelijk is,
 - Ten behoeve van welk samenwerkingsverband de politiegegevens worden verstrekt,
 - Het doel waartoe dit is opgericht,
 - Welke gegevens worden verstrekt,
 - De voorwaarden onder welke de gegevens worden verstrekt en
 - Aan welke personen of instanties de gegevens worden verstrekt.
- De daadwerkelijke verstrekking van gegevens wordt vastgelegd.

24. Rechtstreekse verstrekking

- De organisatie heeft geborgd dat rechtstreekse verstrekking uitsluitend plaatsvindt voor zover noodzakelijk op grond van art 23 en alleen voor zover voldaan kan worden aan de beveiligingseisen.
- De rechtstreekse verstrekking op basis van art 23 lid 2 vindt alleen plaats aan de aangewezen personen.

Onderwerpen en beheersingsmaatregelen
<p>25. Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering</p> <ul style="list-style-type: none"> De verwerkingsverantwoordelijke biedt de betrokkene informatie over de verwerking van persoonsgegevens en doet dit beknopt, toegankelijk en duidelijk, zodat de betrokkene zijn rechten kan uitoefenen. De informatievoorziening voldoet aan de eisen gesteld in art 24b lid 1 en 2. Bij uitstel, beperking of achterwege laten van de verstrekking van informatie bedoeld in 24b lid 2 is de uitstel, beperking of achterwege laten alsmede de duur van deze maatregel onderbouwd. Verzoeken tot inzage, rectificatie, vernietiging van betrokkenen worden - met inachtneming van het gestelde in artikel 27 - tijdig en adequaat afgehandeld. De organisatie borgt dat bij een verzoek tot inzage (art 25 lid 1) of rectificatie (art 28 lid 1) dat de betrokkene zonder onnodige vertraging in kennis wordt gesteld van de ontvangst van het verzoek, de termijn voor uitsluitel en de mogelijkheid een klacht in te dienen bij de AP. Een weigering gevolg te geven aan het verzoek conform art 24a lid 4 is onderbouwd. Elke weigering of beperking van de inzage wordt aan de betrokkene toegelicht, met vermelding van de feitelijke of juridische gronden die aan het besluit ten grondslag liggen.
<p>26. Register</p> <ul style="list-style-type: none"> De verwerkingsverantwoordelijke houdt een register bij dat de gegevens bevat zoals aangegeven in art 31d lid 1. De verwerker houdt een register bij dat de gegevens bevat zoals aangegeven in art 31d lid 2.
<p>27. Documentatie</p> <ul style="list-style-type: none"> De verwerkingsverantwoordelijke borgt een volledige en toegankelijke schriftelijke vastlegging (documentatieplicht) van de onderdelen genoemd in art 32 lid 1. De bedoelde politiegegevens worden conform art 32 lid 4 bewaard. De verwerkingsverantwoordelijke borgt een volledige en toegankelijke schriftelijke vastlegging (documentatieplicht) van de doorgifte van politiegegevens aan een verwerkingsverantwoordelijke in een derde land of aan een internationale organisatie. De schriftelijke melding van een gemeenschappelijke verwerking van politiegegevens aan de AP is geborgd.
<p>28. Logging</p> <ul style="list-style-type: none"> De verwerkingsverantwoordelijke en de verwerker dragen zorg voor de logging van verwerkingen zoals opgenomen in art 32a lid 1. De organisatie gebruikt de logging uitsluitend ter controle van de rechtmatigheid van de gegevensverwerkingen, interne controles, ter waarborging van de integriteit en de beveiliging van politiegegevens en voor strafrechtelijke procedures.
<p>29. Audits</p> <p>Er wordt uitvoering gegeven aan de eisen zoals gesteld in de Regeling periodieke audit politiegegevens.</p>
<p>30. Melding datalekken</p> <ul style="list-style-type: none"> De organisatie detecteert en behandelt privacy gerelateerde incidenten op gepaste wijze om de gevolgen te beperken en maatregelen te nemen om toekomstige inbreuken te voorkomen. De verantwoordelijkheden van de behandeling van datalekken zijn belegd in de organisatie, de daadwerkelijke uitvoering wordt beheerst, gedocumenteerd en geëvalueerd. De melding van een datalek aan de Autoriteit Persoonsgegevens vindt tijdig en volledig plaats. Betrokkenen worden, indien vereist, tijdig en volledig in kennis gesteld van een inbreuk op de beveiliging als deze inbreuk waarschijnlijk een hoog risico voor hun rechten en vrijheden betekent.

Onderwerpen en beheersingsmaatregelen

31. Functionaris voor gegevensbescherming

- Er is een functionaris voor gegevensbescherming aangesteld die toezicht houdt op:
 - het naleven van de Wpg;
 - het beleid van de verwerkingsverantwoordelijke met betrekking tot de bescherming van persoonsgegevens;
 - de toewijzing van de autorisaties, bedoeld in art 6;
 - de bewustmaking en opleiding van de ambtenaren van politie betrokken bij de verwerking van politiegegevens;
 - de audits;
 - de uitvoering van de DPIA's.
- De Functionaris Gegevensbescherming stelt jaarlijks een verslag op van zijn bevindingen en stelt het ter beschikking aan de verwerkingsverantwoordelijke.
- De Functionaris voor Gegevensbescherming is aangemeld bij de Autoriteit Persoonsgegevens.

3 Bevindingen en aanbevelingen

3.1 Algemene bevindingen en aanbevelingen

3.1.1 *Eigenaar/Verantwoordelijkheid*

Vooraf aan de interne audit zijn mede door de inzet van een interim manager diverse acties uitgezet en afgerond die hebben geleid dat verbeteringen zijn gerealiseerd ten aanzien van de Wpg-vereisten voor domein I. Het gevaar is dat vervolgacties en verantwoordelijkheden om aan de Wpg-vereisten te (blijven) voldoen onvoldoende in de organisatie worden verankerd en dat verantwoordelijkheden en overzicht om de naleving hiervan te borgen onvoldoende zijn geformaliseerd. Wij adviseren iemand binnen het domein eigenaar te maken van het handboek en verantwoordelijkheid te geven voor de naleving hiervan.

3.1.2 *Locaties met politiegegevens*

Tijdens de audit werd duidelijk dat Wpg gegevens op meer plekken werden opgeslagen dan alleen de relevante operationele applicaties. Dit betreffen vooral proces verbalen en bezwaren op netwerkschijven en Corsa. Voor de netwerkschijven en Corsa is geen automatische functionaliteit om de bewaartermijnen te handhaven. Dit dient handmatig (bijv. via een periodieke opschoonactie) nageleefd te worden. Ook wordt voor zowel Corsa als de netwerkschijven nog niet aan de loggingvereisten voldaan dat achteraf kan worden vastgesteld wie Wpg-gegevens hebben geraadpleegd. Autorisaties zijn wel ingericht op basis van functievereisten. Wij adviseren om voor Corsa en de netwerkschijven om autorisaties, bewaartermijnen en logging zo adequaat mogelijk te borgen, zodat wordt voldaan aan de vereisten van de Wpg. Voor Corsa adviseren we specifiek om dossiers zonder zaaktype (zoeken op organisatiecode OM) op te schonen of te rubriceren.

3.1.3 *Toetsing werking en auditdossier*

De organisatie moet op dit moment nog een aantal processen en maatregelen beschrijven en formaliseren. Een deel van de processen en geïmplementeerde maatregelen worden al wel uitgevoerd maar zijn niet beschreven (hier wordt op dit moment aan gewerkt). Daarnaast ontbreekt een centraal, gestructureerd auditdossier. Om die reden hebben wij op veel normen de werking niet kunnen toetsen. Wij adviseren bij het beschrijven van processen en maatregelen direct na te denken over hoe de werking van die de maatregelen in die processen in de toekomst kan worden aangetoond.

3.1.4 *Brickyard*

Tijdens de audit zijn aandachtspunten vastgesteld rondom bewaartermijnen in de applicatie Brickyard. De leverancier heeft in 2021 aangegeven dat dit ondersteund zou worden en dat over de interne beheersing en het generieke IT-beheer een TPM zou worden afgegeven. Dit is tot op heden niet gebeurd en wordt nu in de eerste helft van 2024 verwacht. Wij adviseren om hierop toe te zien en met de leverancier hierover nauw in contact te blijven zodat dit voor een volgende audit voldoende wordt geborgd en aangetoond.

3.1.5 IRvN

IRvN heeft een rol ten aanzien van de Wpg doordat zij het beheer op Corsa en de netwerkschijven uitvoeren. Hierdoor zijn de technische maatregelen bij IRvN ook in scope. IRvN is bezig om in de toekomst verantwoording af te leggen over de BIO middels een TPM. In principe zouden de technische maatregelen hierin voldoende onderbouwd moeten zijn. Wij adviseren dit met IRvN af te stemmen en indien nodig aan de zijde van IRvN aanvullende maatregelen in te richten ter ondersteuning van de Wpg-vereisten. Denk bijvoorbeeld aan afschermen van Wpg-gegevens voor medewerkers van IRvN en hierop toezien en wijzigingsbeheer en patchmanagement op Corsa.

3.2 Detailbevindingen en aanbevelingen

In deze bijlage zijn de beheersingsmaatregelen opgenomen zoals die zijn overeengekomen met Gemeente Nijmegen. In de onderstaande tabel hebben wij in de kolom 'Bevindingen' de resultaten van onze werkzaamheden gericht op het vaststellen van de opzet, het bestaan en/of de werking van de beheersingsmaatregelen vastgelegd. In de kolom 'Conclusie / aanbeveling' geven wij aan of aan de criteria voor de opzet, het bestaan en/of de werking wordt voldaan. Daarnaast hebben wij hier ook detailaanbeveling opgenomen.

Onderwerpen	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
1. Reikwijdte (Art 2 lid 1 en 2)	De verwerkingsverantwoordelijke heeft bestanden met politiegegevens binnen de organisatie geïdentificeerd en gedocumenteerd.	Niet in scope van interne audit. Bij initiële audit vorig jaar vastgesteld dat de gemeente een verwerkingsregister heeft opgesteld waarin Wpg verwerkingen zijn opgenomen inclusief de locaties van de bestanden en dat het verwerkingsregister voldoet aan de eisen uit de Wpg. Tevens vastgesteld dat de gemeente een proces heeft opgezet om de actualiteit van het verwerkingsregister te waarborgen.	Niet van toepassing
2. Doelbinding (Art 3 lid 1, 3 en 4, Art 8 lid 1, Art 9 lid 1 en 2, Art 11 lid 1)	Politiegegevens worden alleen verwerkt als dat nodig is voor de in de wet genoemde doeleinden. Geborgd is dat bij het verwerken van politiegegevens altijd sprake is van doelbinding en dat de gegevens niet op een onrechtmatige wijze, worden verwerkt.	Een concept handboek is opgesteld voor Toezicht & Handhaving waarin beknopt uitgangspunten met betrekking tot doelbinding, noodzakelijkheid, rechtmatigheid, juistheid en volledigheid en onderscheid feiten en persoonlijk oordeel zijn opgenomen [35]. De gemeente heeft een proces opgezet waarmee doelbinding wordt getoetst (door de FG) aan de hand van uitgevoerde DPIA's (controle van DPIA's) en daar wordt in het jaarrapportage privacy 2022 over gerapporteerd [103, 108]. Hierin is geconstateerd dat de gemeente sneller en eerder	Voldoet niet Advies: Wij hebben geen actief toezicht vastgesteld ten aanzien van doelbinding (norm 2), noodzakelijkheid (norm 3) en juistheid & volledigheid (norm 4). Wij adviseren de uitgangspunten ten aanzien van toezichtsmaatregelen door FG

Onderwerpen	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
		<p>DPIA's moet uitvoeren, dat is nu in gang gezet. Hiervoor hebben we vastgesteld dat recent een DPIA is geformaliseerd voor applicatie Blackberry Messenger [87]. We hebben vastgesteld dat nog niet voor alle systemen waarin Wpg verwerkingen plaatsvinden een DPIA is uitgevoerd, Een voorbeeld hiervan is Brickyard.</p> <p>Bestudeerde documenten: 87: 20231030_DPIA_BBM-chatapp voor Toezicht en Handhaving.docx 103: 31.4.Uitvoering Controlplan FG Bevindingen Naleving.DEF versie 140222.pdf 35: HANDBOEK TH.v141123-2.docx 108: Jaarrapportage privacy 2022 v1.0.docx noodzakelijkheid en rechtmatigheid, juistheid en volledigheid en onderscheid feit en mening in het kader van de Wpg.</p>	<p>vast te leggen in de handboeken en deze na te leven.</p>
3. Noodzakelijkheid & rechtmatigheid, vermelding herkomst (Art 3 lid 2 en 5)	Er wordt geborgd dat de politiegegevens daartoe toereikend, ter zake dienend en beperkt zijn tot wat noodzakelijk is (niet bovenmatig) en dat de herkomst van gegevens voor art 9 verwerkingen wordt vermeld.	Zie 2.	Voldoet niet
4. Juistheid en volledigheid politiegegevens (Art 4 lid 1)	<p>De verwerkingsverantwoordelijke heeft controles op de kwaliteit ingericht ten behoeve van de borging van de juistheid en nauwkeurigheid van politiegegevens.</p> <p>Er zijn procedures opgesteld voor het vernietigen en rectificeren van politiegegevens.</p>	Zie 2.	Voldoet niet
5. Onderscheid feiten en persoonlijk oordeel (Art 4 lid 3)	Er zijn maatregelen genomen om politiegegevens die op feiten zijn gebaseerd, voor zover mogelijk, te onderscheiden van politiegegevens die op een persoonlijk oordeel zijn gebaseerd.	Zie 2.	<p>Voldoet niet</p> <p>Advies: Wij hebben in het handboek geen uitgangspunten vastgesteld die zorgdragen dat onderscheid</p>

Onderwerpen	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
			tussen feitelijke en subjectieve gegevens wordt gewaarborgd. Wij adviseren dit toe te voegen.
6. Gegevensbescherming door beveiliging en ontwerp (Art 4a lid 1 t/m 5)	<p>Er is (aantoonbaar) een risicoanalyse uitgevoerd waaruit het risiconiveau blijkt en identificeert, evalueert en mitigeert systematisch en periodiek factoren die het beschermen van politiegegevens tegen ongeoorloofde of onrechtmatige verwerking en tegen opzettelijk verlies, vernietiging of beschadiging in gevaar brengen en past de maatregelen hierop aan.</p> <p>De organisatie heeft gegevensbeschermingsbeleid en procedures ontwikkeld en vastgesteld. De verwerkingsverantwoordelijke heeft de maatregelen die nodig zijn om het risico te beperken (passende technische en organisatorische maatregelen) aantoonbaar geïmplementeerd.</p> <p>Privacy by design wordt toegepast/geborgd (bijv. bij ontwikkelingen/ wijzigingen).</p> <p>De verwerkingsverantwoordelijke kan aantonen dat de verwerking van politiegegevens wordt verricht in overeenstemming met wat bepaald is in de wet.</p>	<p>Niet in scope van interne audit.</p> <p>Bij initiële audit vorig jaar vastgesteld dat de gemeente beleid heeft geformaliseerd rondom privacy by design en dat aan de voorkant bij ieder nieuwe intake bij I&A geborgd is dat privacy voldoende onder de aandacht is.</p>	Niet van toepassing
7. Gegevensbescherming door standaardinstellingen (Art 4b lid 1a en lid 1b)	<p>De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen om te waarborgen dat standaard:</p> <p>a) alleen die politiegegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking;</p> <p>b) politiegegevens niet zonder tussenkomst van een natuurlijke persoon voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt.</p>	<p>Niet in scope van interne audit.</p> <p>Bij initiële audit vorig jaar vastgesteld dat de gemeente beleid heeft geformaliseerd rondom privacy by default.</p>	Niet van toepassing

Onderwerpen	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
8. Gegevensbescherming seffectbeoordeling / Data protection impact assessment (DPIA) (Art 4c)	<p>Indien een verwerking waarschijnlijk een hoog risico voor de rechten en vrijheden van personen oplevert worden binnen de organisatie de risico's systematisch geïdentificeerd, beoordeeld en aangepakt door middel van een DPIA die ten minste aan de eisen gesteld in de wet voldoet.</p> <p>De verwerkingsverantwoordelijke beoordeelt, indien nodig of wanneer sprake is van een verandering van het risico, of de verwerking in overeenstemming met de DPIA wordt uitgevoerd en past de DPIA zo nodig aan.</p>	<p>Vastgesteld dat gemeente processen heeft om DPIA's uit te voeren en dat geborgd is in processen dat DPIA's aan de voorkant van het proces worden uitgevoerd [105, 104].</p> <p>We hebben vastgesteld dat recent een DPIA is geformaliseerd voor applicatie Blackberry Messenger [87] en enkele jaren geleden een "Quick PIA" voor Corsa [47, 49, 51]. We hebben vastgesteld dat nog niet voor alle systemen van Toezicht en Handhaving waarin Wpg verwerkingen plaatsvinden een DPIA is uitgevoerd, Een voorbeeld hiervan is Brickyard.</p> <p>Bestudeerde documenten: 105: 1. intakeformulier.pdf 47: 190125 Quickpia Corsa gemeente Nijmegen (1.0).pdf 49: 190125 Quickpia Corsa gemeente Nijmegen (1.0).pptx 104: 2. sjabloon DPIA.docx 87: 20231030_DPIA_BBM-chatapp voor Toezicht en Handhaving.docx 51: Advies Corsa en Privacy.docx</p>	<p>Voldoet niet</p> <p>Advies: Wij adviseren voor alle relevante systemen waarin Wpg-gegevens worden verwerkt een DPIA uit te voeren en toezicht te houden conform de uitgangspunten in de DPIA.</p>
9. Bijzondere categorieën van politiegegevens (Art 5)	<p>Er vindt geen verwerking van bijzondere categorieën van politiegegevens plaats, tenzij:</p> <ul style="list-style-type: none"> - dat onvermijdelijk is voor het doel van de verwerking; - dit in aanvulling is op de verwerking van andere politiegegevens betreffende de persoon; - de gegevens afdoende zijn beveiligd. 	<p>Niet in scope van interne audit.</p> <p>Bijzondere persoonsgegevens zijn uitsluitend van toepassing voor de domeinen Leerrecht en Sociale Recherche en niet van toepassing voor het domein Toezicht en Handhaving.</p>	Niet van toepassing
10. Autorisaties en toegang tot politiegegevens (Art 6 lid 1 t/m 6, Art 6a)	<p>Er is een systeem van autorisaties dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid. Dit houdt in dat: De verwerkingsverantwoordelijke heeft die personen die vanuit hun functie en de wet toegang mogen hebben tot bepaalde politiegegevens geautoriseerd voor alleen die gegevens (need-to-know) .</p> <p>Er is een proces voor het toewijzen, wijzigen en</p>	<p>Een concept handboek is opgesteld voor Toezicht & Handhaving waarin de uitgangspunten voor toegangsbeheer per applicatie vastliggen [35]. Per applicatie zijn autorisatiematrixen opgesteld. Deze zijn in het handboek opgenomen of er wordt verwezen naar een los document [53, 60, 70, 78, 88]</p> <p>Procesmatig is beschreven dat de autorisaties per applicatie meerdere keren per jaar beoordeeld worden. Meest recente</p>	<p>Voldoet niet</p> <p>Advies: In het handboek is nog niet uitgewerkt wie verantwoordelijk is voor het controleren van de autorisaties in CityControl en op welke wijze dit plaatsvindt. Wij adviseren dit nog verder uit te</p>

Onderwerpen	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
	<p>intrekken van autorisaties t.b.v. de toegang tot politiegegevens.</p> <p>Er zijn maatregelen vastgesteld en geïmplementeerd die de identiteit en de toegangsrechten van een gebruiker controleert en rechtmatige toegang tot de gegevens borgt.</p>	<p>autorisatiecontroles liggen niet vast. Deze controles zijn als 0-meting gebruikt voor de nieuwe autorisatiematrixen [66, 81].</p> <p>Via verschillende deelwaarnemingen hebben we voor de relevante applicaties vastgesteld dat de toegang conform de matrix is ingericht:</p> <p>CityControl: Deelwaarneming op adminrechten uitgevoerd. Deze zijn conform de matrix toegekend. Wel zijn er relatief veel accounts met adminrechten. Met name aan de zijde van IRvN.</p> <p>Brickyard: Deelwaarneming op matrix of rechten conform matrix zijn toegekend. Hieruit blijken geen uitzonderingen. Daarnaast de functioneel beheerders beoordeeld. Dit is conform de matrix ingericht en beperkt tot 3 accounts, waarvan één geblokkeerd. Brickyard heeft recent een nieuwe admin-rol toegevoegd. Dit is nog niet verwerkt in de matrix. Dit is een administratieve tekortkoming.</p> <p>Blackberry Messenger: Beheerdersrechten zijn voldoende afgeschermd. Overige medewerkers toegewezen aan één autorisatiegroep. Medewerkertoegang en toestel zijn aan elkaar gekoppeld.</p> <p>Corsa: Autorisaties borgen afgeschermd toegang op zaaktype OM. Meerdere zaken vastgesteld met Wpg gegevens die niet met een dergelijk zaaktype waren geclassificeerd waardoor de toegang te ruim is. De inrichting van de autorisaties sluiten aan bij de matrix.</p> <p>We hebben vastgesteld dat de autorisatiematrixen voldoende actueel zijn en dat autorisaties worden toegekend op basis van functionele behoefte (need to know).</p> <p>Niet-Boa's die toegang krijgen tot Wpg-gegevens dienen een modelverklaring autorisatie niet-Boa te overhandigen. Er moet</p>	<p>werken. Voor sommige applicaties wordt de applicatiebeheerder verantwoordelijk gehouden voor de periodieke controle. Hiermee controleert deze zijn eigen werk. De controle zou beter door een onafhankelijk medewerker gedaan kunnen worden of via een 4-ogenprincipe van twee beheerders. Daarnaast adviseren dat een verantwoordelijk manager kennisneemt van de controle en verantwoordelijkheid neem voor de juistheid van de autorisatie-inrichting.</p> <p>Advies: Periodieke controles dienen minimaal 2 keer per jaar uitgevoerd te worden. Dit is afgelopen jaar nog niet (zichtbaar) gebeurd omdat er eerst een 0-meting is gehouden. Wij adviseren de periodieke controles summier te documenteren: Wie heeft wat wanneer gecontroleerd en wat waren de bevindingen en conclusies.</p> <p>Advies: Op de netwerkschijf van Toezicht & Handhaving is met een zoekactie op Proces Verbalen vastgesteld dat deze in</p>

Onderwerpen	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
		<p>nog eenmalig een controle uitgevoerd worden of de ondertekening van de niet-Boa verklaringen volledig is.</p> <p>Bestudeerde documenten: 70: Autorisatiematrix gezamenlijke map.xlsx 88: Autorisatiematrix BBM UEM.xlsx 78: Autorisatiematrix Brickyard.xlsx 60: Autorisatiematrix City Control 1.1.xlsx 53: Autorisatiematrix Corsa Toezicht en Handhaving.xlsx 81: Gebruikers Brickyard Export.PNG 66: Gebruikers citycontrol export.xlsx 35: HANDBOEK TH.v141123-2.docx</p>	<p>verschillende (archief)mappen verspreid over de afdelingsschijf worden opgeslagen. Wij adviseren hier een eenmalige opschoonactie op alle persoonlijke- en netwerkschijven uit te voeren en vervolgens enkel in de daarvoor bestemde mappen PV's op te slaan, zodat toegang en bewaartermijnen voldoende kunnen worden gehandhaafd.</p> <p>Advies: Wij adviseren autorisaties aan te scherpen in CityControl. Op dit moment hebben meerdere beheerders van IRvN volledige toegang in CityControl en toegang tot Wpg-gegevens, dit zou mogelijk ingeperkt kunnen worden.</p> <p>Advies Periodieke controle op netwerkschijven en Corsa ook uitbreiden door hierin de administrators mee te nemen of deze nog terecht toegang hebben tot Wpg-gegevens.</p>
11 Autorisaties: aanwijzen functionarissen (Art 6 lid 7)	Er is een actuele lijst van, door de verantwoordelijke aangewezen, bevoegde functionarissen.	<p>Niet in scope van interne audit.</p> <p>Artikel 9 onderzoeken zijn uitsluitend van toepassing voor het domein Sociale Recherche en niet van toepassing voor het domein Toezicht en Handhaving.</p>	Niet van toepassing

Onderwerpen	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
12. Onderscheid tussen verschillende categorieën van betrokkenen (Art 6b)	De verwerkingsverantwoordelijke heeft geborgd dat, voor zover mogelijk, duidelijk onderscheid wordt gemaakt in de verschillende categorieën van betrokkenen.	Niet in scope van interne audit. Dit is niet van toepassing voor het domein Toezicht en Handhaving.	Niet van toepassing
13. Verwerker en Verwerkersovereenkomst (Art 6c)	<p>De verwerker stelt de verwerkingsverantwoordelijke alle informatie ter beschikking heeft die nodig is om aantoonbaar te maken dat de verplichtingen in de verwerkersovereenkomst en de Wpg worden nageleefd en die nodig is om audits mogelijk te maken.</p> <p>De verwerking door een verwerker vindt alleen plaats als een verwerkingsverantwoordelijke afdoende garanties heeft over de toereikendheid van de geïmplementeerde technische en organisatorische maatregelen.</p> <p>Bij elke uitvoering van een gegevensverwerking door een verwerker zijn de taken en afspraken schriftelijk vastgesteld en vastgelegd in een (toereikende) overeenkomst of andere rechtshandeling.</p> <p>Er zijn afspraken vastgesteld en vastgelegd m.b.t. de handelswijze bij een inbreuk op de beveiliging.</p> <p>Een andere partij is alleen ingeschakeld bij de uitvoering van de verwerking met toestemming van de verwerkingsverantwoordelijke. Aan deze andere verwerker (subverwerker) is bij een overeenkomst dezelfde verplichtingen inzake gegevensbescherming opgelegd.</p>	<p>Vastgesteld dat de gemeente verwerkersovereenkomsten heeft met alle relevante externe betrokkenen:</p> <ol style="list-style-type: none"> 1. Sigmax (Toezicht & handhaving) [58] 2. Brickyard (Toezicht & handhaving) [75] 3. BlackBerry Messenger [90] 4. Corsa [55] 5. IRvN [106] <p>Wij hebben niet integraal vast kunnen stellen dat alle verwerkers ook aan de contractuele verplichtingen tijdens de verslagperiode hebben voldaan door het ontbreken van TPM's. Sigmax heeft een TPM ter ondersteuning van de Wpg overhandigd, BlackBerry een generieke SOC2 verklaring [91, 92]</p> <p>Bestudeerde documenten:</p> <p>106: 13. Verwerkersovereenkomst IRVN ICT. uitvoering ICT beleid gemeente Nijmegen.pdf</p> <p>75: 13. Verwerkingsovereenkomst Brickyard.handhaving.C01.griftdijk.pdf</p> <p>58: 13.Verwerkersovereenkomst.Sigmax-Citycontrol.Handhaving.pdf</p> <p>91: Blackberry 2023 UEM SOC 2 Report.pdf</p> <p>90: BlackBerry Customer DPA (1.23 Final).pdf</p> <p>92: Toelichting SOC II rapport Blackberry.docx</p> <p>55: Verwerkersovereenkomst.BCT.DMS.systeemCorsa.pdf</p>	<p>Voldoet deels</p> <p>Advies: De naleving van de verwerkersovereenkomsten valt onder het toezicht van de FG. Dit moet voor de applicaties voor domein I nog worden ingericht en uitgevoerd.</p>
14. Geheimhoudingsplicht (Art 7)	Er is geborgd dat de ambtenaar van politie of de persoon aan wie politiegegevens ter beschikking zijn gesteld formeel bekend is met de plicht tot	Een concept handboek is opgesteld voor Toezicht & Handhaving waarin de uitgangspunten ten aanzien van geheimhouding en trainingen uiteen zijn gezet [35]. Een sjabloon	<p>Voldoet deels</p> <p>Advies:</p>

Onderwerpen	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
	geheimhouding en de consequenties bij schending van deze plicht.	<p>geheimhoudingsverklaring is opgenomen in de bijlage [31].</p> <p>Vastgesteld op basis van interview dat gemeenten generiek aandacht aan bewustwording besteden en mensen bij indiensttreden verplicht een geheimhoudingsverklaring laten tekenen en een bewustwordingscursus laten volgen. Daarnaast is er een inwerklijst voor nieuwe medewerkers waar de relevante applicaties en Wpg-regels voldoende onderdeel van zijn [36, 38]. Boa's moeten continu educatie blijven volgen om aangesteld te kunnen blijven als Boa.</p> <p>Verder moeten boa's een opleiding volgen voor zij beëdigd worden waarin aandacht wordt besteed aan dit soort onderwerpen. De gemeente beschikt verder over een sanctiebeleid [107].</p> <p>Bestudeerde documenten: 31: 14. Geheimhoudingsverklaring mei 2019 (2).doc 107: 14. Proces sanctiebeleid en uittreksels personeelshandboek.docx 35: HANDBOEK TH.v141123-2.docx 38: inwerklijst nieuwe medewerkers.docx 36: Leidraad voor leidinggevende Indiensttreding.docx</p>	Wij adviseren bij indiensttreding de checklist zichtbaar af te werken zodat achteraf inzichtelijk is dat alle relevante onderwerpen zijn behandeld, welke ondersteunen aan bewustwording van de Boa.
15. Geautomatiseerde individuele besluitvorming (Art 7a)		Deze norm is alleen van toepassing op de applicatie van Brickyard. Bij herhaling waargenomen dat hierin alleen besluiten mogelijk zijn door middel van menselijke interactie.	Voldoet
16. Uitvoering van de dagelijkse politietaak (Art 8 lid 1 en 2)	Geborgd is dat art 8 politiegegevens één jaar na de datum van de eerste verwerking zodanig worden opgeslagen (achter een schot worden geplaatst) dat ze alleen nog beschikbaar komen voor verdere verwerking op basis van de vergelijking van gegevens (hit-no-hit basis).	Een concept handboek is opgesteld voor Toezicht & Handhaving waarin de uitgangspunten ten aanzien van bewaartermijnen uiteen zijn gezet [35] en halfjaarlijkse controles dienen hierop uitgevoerd worden, Vastgesteld dat gemeente van CityControl gebruikmaakt waarbij de applicatie middels functionaliteit ondersteunt aan de bewaartermijnen, waarmee aan deze norm voldaan kan worden [69]. Blackberry Messenger	Voldoet niet Advies: Voor Corsa en de netwerkschijven adviseren we specifiek beleid te formaliseren om naleving van de

Onderwerpen	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
	Geborgd is voor zover dat noodzakelijk is met het oog op de uitvoering van de dagelijkse politietaak politiegegevens ten aanzien waarvan in art 8 lid 1 genoemde termijn is verstreken geautomatiseerd worden vergeleken met politiegegevens die worden verwerkt op grond van art 8 lid 1 teneinde vast te stellen of verbanden bestaan tussen de betreffende gegevens. De gerelateerde gegevens kunnen verder worden verwerkt met het oog op de uitvoering van de dagelijkse politietaak.	<p>ondersteunt de functionaliteit door berichten na 28 dagen definitief te verwijderen. De werking hiervan is op locatie vastgesteld.</p> <p>Voor andere systemen is dit nog onvoldoende geborgd. In Brickyard is de functionaliteit aanwezig, maar deze werkt nog niet naar behoren. Voor de netwerkschijven is het uitgangspunt dat handmatig de bewaartermijnen geborgd gaan worden. Hier dient nog een corrigerende actie op uitgevoerd te worden. Voor Corsa wordt dit nog verder onderzocht. Hierdoor wordt nog niet volledig voldaan aan deze norm.</p> <p>Bestudeerde documenten: 35: HANDBOEK TH.v141123-2.docx 69: TPM Wpg Sigmax CityControl 2023.pdf</p>	bewaartermijnen te borgen en daarnaast een opschoonactie uit te voeren zodat voldaan wordt aan deze eis.
17. Ter beschikking stellen van politiegegevens binnen het WPG-domein (Art 4 lid 1, Art 8 lid 4, Art 9 lid 3, Art 15 lid 1 en 2)	<p>Geborgd is dat de verdere verwerking van art 9 gegevens alleen plaats vindt na toestemming (aantoonbaar) van de daartoe bevoegde functionaris.</p> <p>Geborgd is dat de ter beschikking stellen van politiegegevens aan bevoegde autoriteiten in andere lidstaten van de Europese Unie of aan organen en instanties belast met de taken, bedoeld in art 1, onderdeel a conform de richtlijnen gesteld in de wet plaatsvindt.</p>	<p>Niet in scope van interne audit.</p> <p>Artikel 9 onderzoeken zijn uitsluitend van toepassing voor het domein Sociale Recherche en niet van toepassing voor het domein Toezicht en Handhaving.</p>	Niet van toepassing
18. Geautomatiseerd vergelijken en in combinatie zoeken (Art 11 lid 1, 3, 4 en 5, Art 8 lid 3, Art 2:1 en 2:2 lid 1 Bpg)	<p>Geborgd is dat gegevens alleen geautomatiseerd worden vergeleken met andere politiegegevens of met andere dan politiegegevens binnen de richtlijnen gesteld in art 11.</p> <p>Geborgd is dat gegevens alleen in combinatie met elkaar worden verwerkt binnen de richtlijnen gesteld in art 11 lid 4.</p>	Deze norm is niet van toepassing voor alle domeinen, dit soort zoekacties vinden niet plaats binnen de gemeente.	Niet van toepassing

Onderwerpen	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
	<p>Geborgd is dat het in combinatie verwerken van art 8 politiegegevens beperkt is tot de ambtenaren van politie die daarvoor geautoriseerd zijn.</p> <p>Geborgd is dat de ambtenaren die geautomatiseerd vergelijken en ambtenaren die in combinatie zoeken over voldoende kennis en vaardigheden beschikken.</p>		
19. Ondersteunende taken (Art 13)	Geborgd is dat voor de verwerkingen bedoeld in art 13 lid 1 t/m 3, van tevoren is voldaan aan de schriftelijke vereisten (art 13 lid 4).	<p>Niet in scope van interne audit.</p> <p>Artikel 13 verwerkingen zijn niet van toepassing.</p>	Niet van toepassing
20. Bewaartermijnen, verwijderen en vernietigen (Art 4 lid 2, Art 8 lid 6, Art 9 lid 4, Art 14)	<p>Politiegegevens worden niet langer bewaard dan de minimale tijd die nodig is, zoals vereist door de toepasselijke wet- en regelgeving, of voor de doeleinden waarvoor deze zijn verwerkt.</p> <p>De verwerkingsverantwoordelijke voorziet in voldoende waarborgen om te bewerkstelligen dat de gegevens conform de wet worden gecontroleerd, verwijderd en vernietigd.</p> <p>Geborgd is dat Politiegegevens na verwijdering maximaal vijf jaar worden bewaard. Indien van cultureel of historisch belang kan worden afgezien van vernietiging van de gegevens. Er wordt dan aan de bewaareisen als genoemd in de Archiefwet voldaan.</p>	Zie norm 16	Voldoet niet
21. Verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee (Art 16, Art 18, Art 19,	<p>Geborgd is dat politiegegevens alleen worden verstrekt aan personen of instanties buiten het politiedomein, voor zover dit noodzakelijk is voor de doeleinden zoals deze in de Wet politiegegevens en het Besluit politiegegevens zijn genoemd.</p> <p>Geborgd is dat wanneer gegevens verstrekt worden</p>	<p>Vastgesteld dat de gemeente over een verstrekkingenwijzer beschikt waarin alle relevante verstrekkingen zijn opgenomen, inclusief hoe verstrekt wordt en waar geregistreerd wordt ten behoeve van de documentatieplicht [39].</p> <p>Bestaan vast kunnen stellen door waarneming in CityControl en Brickyard. Conform de verstrekkingenwijzer dienen alle</p>	<p>Voldoet deels</p> <p>Advies: Het proces rondom het controleren van verstrekkingen formaliseren en minimaal jaarlijks uitvoeren.</p>

Onderwerpen	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
Art 21, Art 22, Art 7 lid 1, Art 4)	<p>er wordt voldaan aan de documentatieplicht (conform 6 lid 4 Bpg).</p> <p>Geborgd is dat verstrekking alleen plaatsvindt in overeenstemming met het bevoegd gezag indien dit vereist is in de wet.</p> <p>Bij verstrekkingen is geborgd dat de ontvangende partij wordt gewezen op zijn geheimhoudingsplicht.</p> <p>De juistheid, volledigheid, actualiteit en betrouwbaarheid van politiegegevens bij verstrekking wordt, voor zover mogelijk, gecontroleerd en inzichtelijk gemaakt voor de ontvangende partij.</p> <p>Er is een procedure voor het onverwijld in kennis stellen van de ontvanger van politiegegevens indien geconstateerd wordt dat onjuiste politiegegevens zijn verstrekt of dat politiegegevens op onrechtmatig wijze zijn verstrekt.</p>	<p>verstrekkingen gedocumenteerd te worden in het Boa Registratie Systeem (BRS). Hier vinden nog geen controles op plaats of dit juist en volledig plaatsvindt.</p> <p>Bestudeerde documenten: 39: Verstrekkingenwijzer.18022022.docx</p>	
22. Doorgiften aan derde landen (Art 17a)	<p>De doorgifte van gegevens aan verwerkingsverantwoordelijke in derde landen vindt alleen plaats indien er een adequaatsheidsbesluit is van de Commissie van de Europese Unie of indien één van de uitzonderingsgronden zoals genoemd in de wet van toepassing is.</p> <p>De doorgifte van gegevens aan derde landen wordt vastgelegd (documentatieplicht).</p> <p>Indien doorgifte plaatsvindt op basis van art 17a lid 2 onderdeel a of b, lid 3 of lid 5 is (aantoonbaar) voldaan aan de gestelde eisen in de wet.</p>	<p>Deze norm is niet van toepassing voor alle domeinen, dit soort verstrekkingen vinden niet plaats binnen de gemeente.</p>	Niet van toepassing

Onderwerpen	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
	<p>De verantwoordelijke heeft inzicht in de samenwerkingsverbanden waarbij politiegegevens worden verstrekt.</p> <p>Indien politiegegevens van een andere lidstaat afkomstig worden doorgegeven aan derde landen is de toestemming van de verantwoordelijke autoriteit van deze lidstaat beschikbaar.</p>		
23. Verstrekking aan derden structureel voor samenwerkingsverbanden (Art 20)	<p>De verantwoordelijke heeft inzicht in de samenwerkingsverbanden waarbij politiegegevens worden verstrekt.</p> <p>In de beslissing voor het verstrekken van politiegegevens t.b.v. een samenwerkingsverband wordt vastgelegd:</p> <ul style="list-style-type: none"> - Ten behoeve van welk zwaarwegend algemeen belang de verstrekking noodzakelijk is, - Ten behoeve van welk samenwerkingsverband de politiegegevens worden verstrekt, - Het doel waartoe dit is opgericht, - Welke gegevens worden verstrekt, - De voorwaarden onder welke de gegevens worden verstrekt en - Aan welke personen of instanties de gegevens worden verstrekt. <p>De daadwerkelijke verstrekking van gegevens wordt vastgelegd.</p>	Zie norm 21	Voldoet deels
24. Rechtstreekse verstrekking (Art 23)	<p>De organisatie heeft geborgd dat rechtstreekse verstrekking uitsluitend plaatsvindt voor zover noodzakelijk op grond van art 23 en alleen voor zover voldaan kan worden aan de beveiligingseisen.</p> <p>De rechtstreekse verstrekking op basis van art 23</p>	Deze norm is niet van toepassing voor alle domeinen, dit soort verstrekkingen vinden niet plaats binnen de gemeente.	Niet van toepassing

Onderwerpen	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
	lid 2 vindt alleen plaats aan de aangewezen personen.		
25. Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering. (Art 24a lid 1 t/m 4, Art 24b, Art 25, Art 26, Art 27, Art 28)	<p>De verwerkingsverantwoordelijke biedt de betrokkene informatie over de verwerking van persoonsgegevens en doet dit beknopt, toegankelijk en duidelijk, zodat de betrokkene zijn rechten kan uitoefenen. De informatievoorziening voldoet aan de eisen gesteld in art 24b lid 1 en 2.</p> <p>Bij uitstel, beperking of achterwege laten van de verstrekking van informatie bedoeld in 24b lid 2 is de uitstel, beperking of achterwege laten alsmede de duur van deze maatregel onderbouwd.</p> <p>Verzoeken tot inzage, rectificatie, vernietiging van betrokkenen worden - met inachtneming van het gestelde in artikel 27 - tijdig en adequaat afgehandeld.</p> <p>De organisatie borgt dat bij een verzoek tot inzage (art 25 lid 1) of rectificatie (art 28 lid 1) dat de betrokkene zonder onnodige vertraging in kennis wordt gesteld van de ontvangst van het verzoek, de termijn voor uitsluitel en de mogelijkheid een klacht in te dienen bij de AP.</p> <p>Een weigering gevolg te geven aan het verzoek conform art 24a lid 4 is onderbouwd. Elke weigering of beperking van de inzage wordt aan de betrokkene toegelicht, met vermelding van de feitelijke of juridische gronden die aan het besluit ten grondslag liggen.</p>	<p>Niet in scope van interne audit.</p> <p>Bij initiële audit vorig jaar vastgesteld dat de gemeente over een privacyverklaring beschikt waarin de Wpg-verwerkingen worden genoemd. Daarnaast beschikt de gemeente over een proces om de rechten van de betrokkenen te behandelen. Alle inzageverzoeken worden geregistreerd.</p>	Niet van toepassing
26. Register (Art 31d lid 1 en 2)	De verwerkingsverantwoordelijke houdt een register bij dat de volgende gegevens bevat: a) de naam en de contactgegevens van de	Niet in scope van interne audit.	Niet van toepassing

Onderwerpen	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
	<p>verwerkingsverantwoordelijke, de gezamenlijk verwerkingsverantwoordelijken en de functionaris voor gegevensbescherming;</p> <p>b) de doelen van de verwerking;</p> <p>c) de categorieën van ontvangers aan wie politiegegevens zijn of zullen worden verstrekt, met inbegrip van ontvangers in derde landen of internationale organisaties;</p> <p>d) een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;</p> <p>e) in voorkomend geval, het gebruik van profilering;</p> <p>f) in voorkomend geval, de categorieën van doorgiften van politiegegevens aan een derde land of een internationale organisatie;</p> <p>g) een aanwijzing van de rechtsgrondslag van de verwerking, met inbegrip van doorgiften, waarvoor de politiegegevens bedoeld zijn;</p> <p>h) zo mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens worden verwijderd of vernietigd;</p> <p>i) zo mogelijk, een algemene beschrijving van de technische en organisatorische maatregelen ter beveiliging, bedoeld in artikel 4a;</p> <p>j) de toekenning van de autorisaties, bedoeld in artikel 6.</p> <p>De verwerker houdt een register bij dat de volgende gegevens bevat:</p> <p>a) de naam en de contactgegevens van de verwerker of verwerkers en van iedere verwerkingsverantwoordelijke ten behoeve van wie de verwerker handelt en, in voorkomend geval, van de functionaris voor gegevensbescherming;</p> <p>b) de categorieën van verwerkingen die namens iedere verwerkingsverantwoordelijke zijn</p>	<p>Bij initiële audit vorig jaar vastgesteld dat de gemeente een verwerkingsregister heeft opgesteld waarin Wpg-verwerkingen zijn opgenomen inclusief de locaties van de bestanden en dat het verwerkingsregister voldoet aan de eisen uit de Wpg.</p> <p>Tevens vastgesteld dat de gemeente een proces heeft opgezet om de actualiteit van het verwerkingsregister te waarborgen.</p>	

Onderwerpen	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
	<p>uitgevoerd;</p> <p>c) indien van toepassing, doorgiften van politiegegevens aan een derde land of een internationale organisatie, onder vermelding van dat derde land of die internationale organisatie, indien door de verwerkingsverantwoordelijke uitdrukkelijk daartoe geïnstrueerd</p> <p>d) indien mogelijk, een algemene beschrijving van de technische en organisatorische maatregelen, bedoeld in artikel 4a.</p>		
27. Documentatie (Art 32 lid 1 t/m 4)	<p>De verwerkingsverantwoordelijke borgt een volledige en toegankelijke schriftelijke vastlegging (documentatieplicht) van de onderdelen genoemd in art 32 lid 1. De bedoelde politiegegevens worden conform art 32 lid 4 bewaard.</p> <p>De verwerkingsverantwoordelijke borgt een volledige en toegankelijke schriftelijke vastlegging (documentatieplicht) van de doorgifte van politiegegevens aan een verwerkingsverantwoordelijke in een derde land of aan een internationale organisatie.</p> <p>De schriftelijke melding van een gemeenschappelijke verwerking van politiegegevens aan de AP is geborgd.</p>	<p>1. Registratie artikel 9 doeleinden: n.v.t.</p> <p>2. Registratie verstrekkingen: Zie norm 21</p> <p>3. Registratie afwijzingen: zie norm 25</p> <p>4. Registratie datalekken: zie norm 30</p>	Voldoet deels
28. Logging (Art 32a)	<p>De verwerkingsverantwoordelijke en de verwerker dragen zorg voor de logging van verwerkingen zoals opgenomen in art 32a lid 1.</p> <p>De organisatie gebruikt de logging uitsluitend ter controle van de rechtmatigheid van de gegevensverwerkingen, interne controles, ter waarborging van de integriteit en de beveiliging van politiegegevens en voor strafrechtelijke procedures</p>	Een concept handboek is opgesteld voor Toezicht & Handhaving waarin uitgangspunten met betrekking tot beoordeling van de logging zijn vastgelegd [35]. Er is momenteel sprake van logging in de systemen CityControl, Blackberry Messenger en Brickyard. Logging die bruikbaar is voor onderzoek en analyse dient bij de leverancier te worden opgevraagd. CityControl ondersteunt de betrouwbaarheid van de logging met haar TPM [69, 68]. De organisatie is nog zoekende om effectieve logcontroles uit te voeren. Voor	<p>Voldoet niet</p> <p>Advies: Het onderdeel loggingcontrole dient nog verder uitgewerkt te worden in het handboek. Daarnaast dienen logcontroles (behalve Brickyard) nog uitgevoerd te worden.</p>

Onderwerpen	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
		<p>Brickyard ligt dit vast [86]. Verder worden zaken opgeslagen in Corsa en op de netwerkschijf. Logging hierin is technisch mogelijk, maar kent nu nog beperkingen omdat logging op raadplegen niet is ingericht. Er wordt nog gekeken naar een wijze voor totale controle van logging.</p> <p>Bestaan vastgesteld dat voor een log-controle welke is uitgevoerd voor Brickyard. Hierbij is onderzoek gedaan naar PV's die meerdere keren zijn bekeken [79, 83]. Aanvullend tijdens de audit ook nog in de logging de mutaties beoordeeld van accounts die geen mutaties horen te doen, hieruit bleken geen uitzonderingen.</p> <p>Bestudeerde documenten: 79: Controle log Brickyard 02-2023 tm 07-2023.docx 35: HANDBOEK TH.v141123-2.docx 83: nijmegen-audit-log Brickyard.xlsx 68: Toelichting logging Citycontrol.docx 69: TPM Wpg Sigmax CityControl 2023.pdf 86: Werkwijze controle log Brickyard.docx</p>	
29. Audits (Art 33)	Er wordt uitvoering gegeven aan de eisen zoals gesteld in de Regeling Periodieke Audit politiegegevens.	<p>De gemeente heeft in 2022 een interne audit uitgevoerd [102]. De beoogde interne auditor is vertrokken bij gemeente Nijmegen waardoor in 2023 2-Control de interne audit heeft uitgevoerd.</p> <p>Conform de auditplanning in het rapport van 2022 is domein I in scope van de interne audit 2023 [102]. Dit is conform auditplanning uitgevoerd.</p> <p>Bestudeerde documenten: 102: Wpg-intern-2022 Interne audit Wet Politiegegevens Gemeente Nijmegen - DEFINITIEF.pdf</p>	Voldoet
30. Melding datalekken (Art 33a)	De organisatie detecteert en behandelt privacy gerelateerde incidenten op gepaste wijze om de gevolgen te beperken en maatregelen te nemen om	<p>Niet in scope van interne audit.</p> <p>Bij initiële audit vorig jaar vastgesteld dat de gemeente over een</p>	Niet van toepassing

Onderwerpen	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
	<p>toekomstige inbreuken te voorkomen.</p> <p>De verantwoordelijkheden van de behandeling van datalekken zijn belegd in de organisatie, de daadwerkelijke uitvoering wordt beheerst, gedocumenteerd en geëvalueerd.</p> <p>De melding van een datalek aan de AP vindt tijdig en volledig plaats.</p> <p>Betrokkenen worden, indien vereist, tijdig en volledig in kennis gesteld van een inbreuk op de beveiliging als deze inbreuk waarschijnlijk een hoog risico voor hun rechten en vrijheden betekent.</p>	<p>procedure datalekken beschikt en een register bijhoudt en voorbeelden ingezien.</p>	
31. Functionaris voor gegevensbescherming (Art 36)	<p>Er is een functionaris voor gegevensbescherming aangesteld die toezicht houdt op:</p> <ul style="list-style-type: none"> - het naleven van de Wpg; - het beleid van de verwerkingsverantwoordelijke met betrekking tot de bescherming van persoonsgegevens; - de toewijzing van de autorisaties, bedoeld in art 6; - de bewustmaking en opleiding van de ambtenaren van politie betrokken bij de verwerking van politiegegevens; - de audits; - de uitvoering van de DPIA's. <p>De FG stelt jaarlijks een verslag op van zijn bevindingen en stelt het ter beschikking aan de verwerkingsverantwoordelijke.</p> <p>De functionaris voor gegevensbescherming is aangemeld bij de Autoriteit Persoonsgegevens en de contactgegevens van de FG zijn openbaar gemaakt.</p>	<p>Vastgesteld dat de gemeente een FG heeft aangesteld [109]. Vastgesteld dat de FG jaarlijks toezicht houdt op diverse onderdelen [103]. Het controleplan bestaat uit meerdere onderdelen:</p> <ul style="list-style-type: none"> • AVG proof zijn van alle afdelingen (inzicht en beheersing van verwerking persoonsgegevens) • Datalekken en privacykwesties • DPIA's en naleving • Verwerkersovereenkomsten (naleving) • Privacy Protocol. <p>Bestaan van jaarlijks toezicht vastgesteld aan de hand van jaarrapportage privacy 2022 [108].</p> <p>We hebben vastgesteld dat nog niet voor alle systemen van Toezicht en Handhaving waarin Wpg verwerkingen plaatsvinden een DPIA is uitgevoerd, Een voorbeeld hiervan is Brickyard.</p> <p>Bestudeerde documenten: 103: 31.4.Uitvoering Controlplan FG Bevindingen Naleving.DEF versie 140222.pdf</p>	<p>Voldoet niet</p> <p>Advies: Wij adviseren voor alle relevante systemen waarin Wpg gegevens worden verwerkt een DPIA uit te voeren en toezicht te houden conform de uitgangspunten in de DPIA.</p>

Onderwerpen	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
		109: 31.aanmelding FG (Nijmegen).pdf 108: Jaarrapportage privacy 2022 v1.0.docx	

3.3 Detailbevindingen en aanbevelingen technische en organisatorische maatregelen

Gemeente Nijmegen maakt voor deze verwerkingen gebruik van de volgende informatiesystemen:

Processen/verwerkingen	Informatiesysteem	Beheerorganisatie	Leverancier
Opsporing strafbare feiten in domein I (openbare ruimte)	CityControl	Sigmax	Sigmax
Opsporing strafbare feiten in domein I (openbare ruimte)	Brickyard (C1)	Brickyard	Brickyard
Opsporing strafbare feiten in domein I (openbare ruimte)	Blackberry Messenger	Blackberry	Blackberry
Opsporing strafbare feiten in domein I (openbare ruimte)	Netwerkschijf	IRvN	N.V.T.
Opsporing strafbare feiten in domein I (openbare ruimte)	Corsa	IRvN	BCT

Onderwerp	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
GITC01. Wijzigingenbeheer	<p>Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.</p> <p>Doelstelling: Zeker stellen dat wijzigingen op een correcte en gecontroleerde wijze worden doorgevoerd waardoor de veilige werking van ICT-voorziening wordt gegarandeerd.</p> <p>Scope: Applicatie-, hosting (verwerker)- of SAAS leverancier van de Wpg-geclassificeerde verwerkende systemen.</p>	<p>Wij hebben niet integraal vast kunnen stellen dat alle verwerkers ook aan de technische vereisten tijdens de verslagperiode hebben voldaan door het ontbreken van TPM's. Sigmax heeft een TPM ter ondersteuning van de Wpg overhandigd [69]. Op basis hiervan wordt voldaan aan deze norm, BlackBerry overhandigt een generieke SOC2 verklaring waarin deze norm voldoende wordt ondersteund [91,92]. Brickyard verwacht in 2024 een TPM te kunnen verstrekken [85].</p> <p>Vastgesteld dat de IRvN een procedure Wijzigingsbeheer heeft [110]. Bestaan vastgesteld aan de hand van twee voorbeelden (Corsa en een technische wijziging) [111, 112]. Voor alle wijzigingsverzoeken op Corsa moet gemeente Nijmegen daar voor tekenen. Updates komen ongeveer iedere 2 jaar uit. Patches (Service Pack) komen ongeveer maandelijks uit maar worden maar 1 à 2 keer per jaar doorgevoerd. Leverancier</p>	<p>Voldoet deels</p> <p>Advies (voor alle GITC-normen) Bij Brickyard toe te zien dat er een TPM komt waarin aan deze normen wordt voldaan. Daarnaast adviseren we met IRvN afspraken te maken hoe zij aantoonbaar kunnen voldoen aan deze vereisten onderliggend aan het netwerk en Corsa. Dit zou in de toekomst via een TPM geborgd gaan worden, in de tussentijd is het essentieel dat IRvN dit voldoende aan kan tonen aan de gemeente Nijmegen.</p>

Onderwerp	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
		<p>(BCT) installeert updates i.v.m. complexiteit door koppelingen.</p> <p>Bestudeerde documenten: 110: 10.1.2 Procedure Wijzingsbeheer.docx 91: Blackberry 2023 UEM SOC 2 Report.pdf 92: Toelichting SOC II rapport Blackberry.docx 69: TPM Wpg Sigmax CityControl 2023.pdf 111: W2107 1421 upgrade Corsa testomgevingpdf.pdf 112: W2303 0490 update citrix license server.pdf 85: Wpg-verklaring plus audit Versie 1.1_17112021_BY_FT.pdf</p>	
GITC02. Logische toegangsbeveiliging	<p>De inzet van identiteit- en toegangsmiddelen levert betrouwbare en effectieve mechanismen voor het vastleggen en vaststellen van de identiteit van gebruikers, het toekennen van de rechten aan gebruikers, het controleerbaar maken van het gebruik van deze middelen en het automatiseren van arbeidsintensieve taken.</p> <p>Doelstelling: Het efficiënter maken van het identiteit- en toegangsbeheer en zorgen dat functies en gegevens uitsluitend beschikbaar worden gesteld aan diegenen waarvoor deze bedoeld zijn als waarborg voor vertrouwelijkheid en integriteit.</p> <p>Scope: Hosting, leverancier van de Wpg-geclassificeerde verwerkende systemen.</p>	<p>Wij hebben niet integraal vast kunnen stellen dat alle verwerkers ook aan de technische vereisten tijdens de verslagperiode hebben voldaan door het ontbreken van TPM's. Sigmax heeft een TPM ter ondersteuning van de Wpg overhandigd [69]. Op basis hiervan wordt voldaan aan deze norm, BlackBerry overhandigt een generieke SOC2 verklaring waarin deze norm voldoende wordt ondersteund [91,92]. Brickyard verwacht in 2024 een TPM te kunnen verstrekken [85]. Wachtwoordbeheer van Brickyard is verder onderzocht tijdens de audit. De complexiteit van wachtwoorden wordt geborgd. Het is onbekend of periodiek wijzigen en MFA worden ondersteund [84].</p> <p>Vastgesteld dat IRvN procedures heeft voor instroom, doorstroom en uitstroom van medewerkers [113, 114]. Bestaan vastgesteld aan de hand van voorbeelden indienst 5.1.2e [115], uit dienst 5.1.2e [116] en mutatie 5.1.2e [117].</p> <p>Bestudeerde documenten: 91: Blackberry 2023 UEM SOC 2 Report.pdf 113: Instroom medewerker processtappen.docx 92: Toelichting SOC II rapport Blackberry.docx 69: TPM Wpg Sigmax CityControl 2023.pdf 114: Uitstroom medewerker processtappen.docx</p>	Voldoet deels

Onderwerp	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
		<p>115: W2203 1465 account IRVN aanmaken.pdf 116: W2210 1424 account irvn verwijderen.pdf 117: W2301 0024 account mutatie 5.1.2e .pdf 84: Wachtwoordbeleid Brickyard.PNG 85: Wpg-verklaring plus audit Versie 1.1_17112021_BY_FT.pdf</p>	
GITC03. Beheer van kwetsbaarheden (patchmanagement)	<p>Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt behoort tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden te worden geëvalueerd en passende maatregelen te worden genomen om het risico dat ermee samenhangt aan te pakken.</p> <p>Doelstelling: Zeker stellen dat technische en software kwetsbaarheden tijdig en effectief worden aangepakt en zo een stabiele omgeving wordt gecreëerd.</p> <p>Scope: Hosting, leverancier van de Wpg-geclassificeerde verwerkende systemen.</p>	<p>Wij hebben niet integraal vast kunnen stellen dat alle verwerkers ook aan de technische vereisten tijdens de verslagperiode hebben voldaan door het ontbreken van TPM's. Sigmax heeft een TPM ter ondersteuning van de Wpg overhandigd [69]. Op basis hiervan wordt voldaan aan deze norm, BlackBerry overhandigt een generieke SOC2 verklaring waarin deze norm voldoende wordt ondersteund [91,92]. Brickyard verwacht in 2024 een TPM te kunnen verstrekken [85]. Wachtwoordbeheer verder onderzocht tijdens de audit. De complexiteit van wachtwoorden wordt geborgd. Het is onbekend of periodiek wijzigen en MFA worden ondersteund.</p> <p>Ten aanzien van Corsa zie GITC01.</p> <p>Bestudeerde documenten: 91: Blackberry 2023 UEM SOC 2 Report.pdf 92: Toelichting SOC II rapport Blackberry.docx 69: TPM Wpg Sigmax CityControl 2023.pdf 85: Wpg-verklaring plus audit Versie 1.1_17112021_BY_FT.pdf</p>	Voldoet deels
GITC04. Cryptografie	<p>Ter bescherming van politiegegevens behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.</p> <p>Doelstelling: Zorgen voor correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en/of integriteit van politiegegevens te beschermen.</p>	<p>Wij hebben niet integraal vast kunnen stellen dat alle verwerkers ook aan de technische vereisten tijdens de verslagperiode hebben voldaan door het ontbreken van TPM's. Sigmax heeft een TPM ter ondersteuning van de Wpg overhandigd [69]. Op basis hiervan wordt voldaan aan deze norm, BlackBerry overhandigt een generieke SOC2 verklaring waarin deze norm voldoende wordt ondersteund [91,92]. Brickyard verwacht in 2024 een TPM te kunnen verstrekken [85]. Wachtwoordbeheer verder onderzocht tijdens de audit. De complexiteit van wachtwoorden wordt geborgd. Het is onbekend of periodiek wijzigen en MFA worden ondersteund.</p>	Voldoet deels

Onderwerp	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
	<p>Scope: Hosting, leverancier van de Wpg-geclassificeerde verwerkende systemen.</p>	<p>IRvN heeft voor Corsa geen specifieke cryptografische maatregelen getroffen. Dit is in deze interne audit niet verder onderzocht.</p> <p>Bestudeerde documenten: 91: Blackberry 2023 UEM SOC 2 Report.pdf 92: Toelichting SOC II rapport Blackberry.docx 69: TPM Wpg Sigmax CityControl 2023.pdf 85: Wpg-verklaring plus audit Versie 1.1_17112021_BY_FT.pdf</p>	
GITC05. Vulnerability scans en Penetratietesten	<p>Penetratietesten en vulnerability scans worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de systemen waarin politiegegevens verwerkt worden.</p> <p>Doelstelling: Het verkrijgen van inzicht in de weerstand die de systemen kunnen bieden aan pogingen om het te compromitteren.</p> <p>Scope: Hosting, leverancier van de Wpg-geclassificeerde verwerkende systemen.</p>	<p>Wij hebben niet integraal vast kunnen stellen dat alle verwerkers ook aan de technische vereisten tijdens de verslagperiode hebben voldaan door het ontbreken van TPM's. Sigmax heeft een TPM ter ondersteuning van de Wpg overhandigd [69]. Op basis hiervan wordt voldaan aan deze norm, BlackBerry overhandigt een generieke SOC2 verklaring waarin deze norm voldoende wordt ondersteund [91,92]. Brickyard verwacht in 2024 een TPM te kunnen verstrekken [85]. Wachtwoordbeheer verder onderzocht tijdens de audit. De complexiteit van wachtwoorden wordt geborgd. Het is onbekend of periodiek wijzigen en MFA worden ondersteund.</p> <p>IRvN heeft een Vulnerability management beleid. In dit beleid zijn de uitgangspunten opgesteld ten aanzien van kwetsbaarhedenbeheer en de opvolging van kwetsbaarheden. Dit is in deze interne audit niet verder onderzocht.</p> <p>Bestudeerde documenten: 91: Blackberry 2023 UEM SOC 2 Report.pdf 92: Toelichting SOC II rapport Blackberry.docx 69: TPM Wpg Sigmax CityControl 2023.pdf 85: Wpg-verklaring plus audit Versie 1.1_17112021_BY_FT.pdf</p>	Voldoet deels

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, 6, 22, 34, 35