VERBETERRAPPORT AUDIT WET POLITIEGEGEVENS

INHOUDSOPGAVE

INLEIDING

Als een Buitengewoon opsporingsambtenaar (boa) persoonsgegevens verwerkt zijn er twee wettelijke regimes van toepassing. Persoonsgegevens die een boa verwerkt in zijn rol als toezichthouder, vallen onder de AVG. De gegevens die de boa als opsporingsambtenaar verwerkt, vallen onder de Wet politiegegevens (Wpg). Voor gegevens die onder de Wpg worden verwerkt (voor opsporing dus), gelden andere regels dan onder de AVG het geval zou zijn geweest. Bijvoorbeeld andere bewaartermijnen, of andere eisen die gelden bij het onderling delen van gegevens. Om vast te kunnen stellen dat gemeenten – waaronder de gemeente Venlo - de verwerkingen van persoonsgegevens die onder de Wpg vallen conform de wettelijke eisen hebben toegepast, wordt de audit Wet politiegegevens uitgevoerd.

Volgens de Wpg dient 'de verwerkingsverantwoordelijke' een interne audit en eenmaal in de vier jaren een externe privacy audit uit te voeren. Die interne audit is te vergelijken met een zelfevaluatie. De interne audit heeft betrekking op enkele onderdelen van de wet en heeft tot doel voor het onderdeel of de onderdelen van de wet waar de interne audit zich op richt, op systematische wijze te toetsen of aan de bepalingen van de wet op adequate wijze uitvoering is gegeven. In onderstaand overzicht staan de wettelijke verplichtingen die voortvloeien uit de verantwoordingsplicht kort samengevat.

Eens per jaar een interne audit uitvoeren (artikel 3 Regeling periodieke audit politiegegevens)

Twee jaar na invoering wet en vervolgens eens per vier jaar een externe audit uitvoeren. Auditrapport verstrekken aan AP (artikel 6:5 Besluit politiegegevens en artikel 33 Wet politiegegevens).

Audit niet op alle fronten in orde? Binnen 3 maanden een verbeterrapport opstellen en binnen een jaar een hercontrole uitvoeren (artikel 4 Regeling periodieke audit politiegegevens). Ook die resultaten moeten aan de AP verstrekt worden (artikel 33 Wet politiegegevens) .

Net als andere gemeenten verwerkt ook de gemeente Venlo bij het uitvoeren van enkele taken politiegegevens. **De gemeente Venlo verwerkt politiegegevens in de domeinen 1, 2, 3 en 5.**

Domein	Boa-werkterrein	Organisatie onderdeel
1	Openbare ruimte	Team Handhaving en wijkgericht werken
2	Milieu, welzijn en infrastructuur	Team Toezicht en handhaving Milieu en bodem
3	Onderwijs	Leerplicht RMC Werk
4	Openbaar Vervoer	n.v.t.
5	Werk, inkomen en zorg	Team Werk Sociale Recherche
6	Generieke opsporing	n.v.t.

In 2022 is een interne audit en een externe audit uitgevoerd. Na de interne audit zijn maatregelen getroffen om aan de normen te voldoen. Uit de externe audit bleek dat de gemeente daardoor aan (veel) meer normen voldoet, maar ook dat de gemeente nog niet voldoet aan alle normen. Het is wettelijk verplicht (artikel 4 lid 1 regeling periodieke audit politiegegevens) dat na de externe audit een verbeterrapport wordt opgesteld en eind 2023 een hercontrole moet zijn uitgevoerd (door een externe auditor) waarvan de

resultaten uiterlijk 31 december 2023 verstrekt moeten worden aan de Autoriteit Persoonsgegevens.

Dit verbeterrapport audit Wet politiegegevens is gemaakt om te ondersteunen bij het organiseren van deze verantwoording over de privacy en informatiebeveiliging bij het verwerken van politiegegevens. In dit verbeterrapport is aan de hand van de resultaten van de externe audit per domein een actieplan opgesteld. Daarin is ook in de legenda het onderscheid gemaakt tussen opzet, bestaan en werking van een beheersmaatregel. Daarbij wordt aangesloten bij de externe audit. De ambitie is om de beheersmaatregelen te treffen die nodig zijn om aan de normen van de Wpg te voldoen. Dat kan niet in één keer. Daarom is een risico gebaseerde planning opgesteld voor het uitvoeren van de maatregelen. Zie de tabel hieronder.

Onderwerpen	Risico (H/M/L)	Motivering	Planning		
			2023	2024	2025
1. Reikwijdte	Midden	De vastlegging van de bestanden met politiegegevens vindt in 2023 plaats ihkv actualisering van het register van verwerkingen. Periodieke controle op de actualiteit ervan (dat is de beheersactie die voortvloeit uit de Wpg audit) vindt daarna jaarlijks plaats als onderdeel van het beheer van het register van verwerkingen.		x	x
2. Doelbinding	Midden	De vastlegging van de bestanden met politiegegevens vindt in 2023 plaats ihkv actualisering van het register van verwerkingen. Periodieke controle op de actualiteit ervan (dat is de beheersactie die voortvloeit uit de Wpg audit) vindt daarna jaarlijks plaats als onderdeel van het beheer van het register van verwerkingen.		x	x
3. Noodzakelijkheid en rechtmatigheid, vermelding herkomst	Midden	De vastlegging van noodzakelijkheid en rechtmatigheid en de vermelding van de herkomst vindt in 2023 plaats in het kader van de DPIA. Periodieke controles op noodzakelijkheid en toereikendheid en op welke dossiers de controles zijn uitgevoerd (dat is de beheersactie die voortvloeit uit de Wpg audit) vindt daarna jaarlijks plaats.	x	x	x
4. Juistheid en volledigheid politiegegevens	Hoog	Periodieke controle op de kwaliteit ingericht ten behoeve van de borging van de juistheid	x		

Onderwerpen	Risico (H/M/L)	Motivering	Planning		
			2023	2024	2025
		en nauwkeurigheid van politiegegevens en het opstellen van procedures voor vernietiging en rectificeren van politiegegevens bestaat nog niet en is nog niet werkend. Hoge impact voor betrokkenen indien dit fout gaat.			
5. Onderscheid feiten en oordeel	Laag	Er zijn al maatregelen genomen om politiegegevens die op feiten zijn gebaseerd, voor zover mogelijk, te onderscheiden van politiegegevens die op een persoonlijk oordeel zijn gebaseerd. Borging hiervan is nog niet geregeld.			x
6. Gegevensbescherming door beveiliging en ontwerp	Midden	Periodieke controle uit op autorisaties en logging v.w.b.t. verlies/vernietiging/ beschadiging volgt als de autorisaties en logging is geregeld in 2023 en 2024		x	
7. Gegevensbescherming door standaardinstellingen	Midden	Technische en organisatorische maatregelen worden deels al in 2023 aangetoond door andere maatregelen uit te voeren. Daardoor van Hoog naar Midden-risico		x	
8. Gegevensbeschermingseffectbeoordeling/ Data protection impact assessment (DPIA)	Hoog	Geeft risico's aan in de verwerking, nodig ivm accountability en opgenomen in al vastgestelde DPIA planning	x		
9. Bijzondere categorieën van politiegegevens	Midden	Deze worden niet verwerkt. Borging is niet geregeld (bijv. door steekproeven op dossiers)		x	
10. Autorisaties en toegang tot politiegegevens	Hoog	Niet geborgd is wie toegang heeft tot de politiegegevens vlgs de Wpg audit	x		
11. Autorisaties: aanwijzen functionarissen	Laag	Er vinden nog geen art. 9 Wpg verwerkingen plaats			x
12. Onderscheid tussen verschillende categorieën van betrokkenen	Hoog	Geen (voldoende) zicht op welke persoonsgegevens van welke categorie betrokkenen wordt verwerkt.	x		
13. Verwerker en Verwerkersovereenkomst	Hoog	Afspraken ivm gebruik en beveiliging van applicaties (indien van toepassing)	x		
14. Geheimhoudingsplicht	Midden	Opleidingen Boa's moet geregeld en aangetoond worden m.b.t. Wpg		x	
15. Geautomatiseerde individuele besluitvorming	Laag	Aan normen wordt voldaan. In 2025 volgt herhaald onderzoek.			x

Onderwerpen	Risico (H/M/L)	Motivering	Planning		
			2023	2024	2025
16. Uitvoering van de dagelijkse politietaak	Midden	Zorg voor de implementatie van het achter schot plaatsen van politiegegevens in de applicatie na 1 jaar, waarna ze enkel nog beschikbaar zijn op hit-no-hit basis is nodig om niet meer gegevens beschikbaar te hebben dan strikt nodig. Dit houdt verband met de bewaartermijnen		x	
17. Ter beschikking stellen van politie-gegevens binnen het WPG-domein	Laag	Dit gebeurt nu niet.			x
18. Geautomatiseerd vergelijken en in combinatie zoeken	Laag	Politiegegevens kunnen worden vergeleken met andere politiegegevens met als doel om vast te stellen of verbanden bestaan tussen de betreffende gegevens. De verwerkingsmogelijkheden geautomatiseerd vergelijken en in combinatie zoeken zijn gebonden aan strikte criteria. Vlgs Wpg audit voldoet Venlo aan de norm vwb opzet en bestaan. Aandacht nodig voor de werking ervan			x
19. Ondersteunende taken	Laag	Vooralsnog zijn er geen gevallen bekend van artikel 13-verwerkingen voor Boa's. Er wordt verwacht dat dit in de toekomst wel gaat gebeuren.			x
20. Bewaartermijnen, verwijderen en vernietigen	Hoog	Politiegegevens mogen niet langer worden bewaard dan is vastgelegd in wet- en regelgeving, of voor de doeleinden waarvoor deze zijn verwerkt. Dit is nog niet goed geregeld (opzet deels geregeld, bestaan en werking niet). Groot risico m.b.t. evt. datalek, dataminimalisatie.	x		
21. Verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee	Hoog	Het onterecht of op onjuiste wijze verstrekken van politiegegevens kan een hoog risico voor betrokkenen vormen. De kans hierop neemt toe indien dit niet goed is beschreven en geborgd.	x		
22. Doorgiften aan derde landen	Laag	Vindt op dit moment niet plaats			x
23. Verstrekking aan derden structureel voor samenwerkingsverbanden	Hoog	Stel vast of en documenteer welke samenwerkingsverbanden bestaan waarbij politiegegevens worden verstrekt zoals bedoeld in artikel 20 (betreffende organisaties die niet in het Besluit	x		

Onderwerpen	Risico (H/M/L)	Motivering	Planning		
			2023	2024	2025
		politiegegevens zijn opgenomen). Het onterecht of op onjuiste wijze verstrekken van politiegegevens kan een hoog risico voor betrokkenen vormen. De kans hierop neemt toe indien dit niet goed is beschreven en geborgd.			
24. Rechtstreekse verstrekking	Laag	Dit gebeurt op dit moment niet			x
25. Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering	Laag	Van groot belang voor betrokkenen, maar is al in orde voor opzet en bestaan vlgs Wpg audit. Betreft vastlegging waaruit blijkt dat in de loop der jaren de privacyverklaring beschikbaar is op de website en dat uitvoering van de procedure rechten van betrokkenen aantoonbaar is uitgevoerd. Wordt al aangetoond door de heraudit en het jaarverslag van de FG		x	x
26. Register	Hoog	Zonder actueel register van verwerkingen dat voldoet aan de eisen van de Wpg is de uitvoering van andere maatregelen niet mogelijk. Het is de basis voor de verwerking van politiegegevens.	x		
27. Documentatie	Midden	De verwerkingsverantwoordelijke heeft een documentatieplicht. De documentatieplicht heeft niet alleen als doel het afleggen van verantwoording, maar ook het creëren van transparantie rondom de gegevensverwerkingen.		x	
28. Logging	Midden	Is nog niet geregeld in de wet, wel wenselijk		x	
29. Audits	Laag	Door de interne, her- en externe audits uit te voeren wordt voldaan aan de norm	x	x	x
30. Melding datalekken	Laag	Er wordt aan de norm voldaan			x
31. Functionaris voor Gegevensbescherming	Laag	Door toezicht vorm te geven wordt aan deze norm voldaan	x	x	x
Technische en organisatorische maatregelen					
1. Wijzigingenbeheer	Midden	Toon aan dat het wijzigingenbeheer wordt uitgevoerd voor de applicatie die wordt gebruikt. Dit kan nl. gevolgen hebben voor de beveiliging van de persoonsgegevens. Opzet en bestaan is al in orde.		x	

Onderwerpen	Risico (H/M/L)	Motivering	Planning		
			2023	2024	2025
2. Logische toegangsbeveiliging	Midden	Autorisaties moeten geborgd zijn. Daarvoor is een autorisatieprocedure nodig die ook bekend is en wordt toegepast. Alleen dan is er een aantoonbaar kader voor het verlenen in intrekken van autorisaties.		x	
3. Beheer van kwetsbaarheden (patchmanagement)	Midden	Patchmanagement moet aanwezig zijn incl. een aantoonbaar kader hiervoor en de borging ervan		x	
4. Cryptografie	Midden	Beveiligingsmaatregel. Toon aan dat cryptografiebeleid van de gemeente wordt toegepast voor de applicaties die wordt gebruikt		x	
5. Vulnerability scans en Penetratietesten	Midden	De beveiliging van de applicaties moet in orde zijn. Dat hoeft niet jaarlijks te worden getest, maar wel regulier om zeker te zijn van mogelijke kwetsbaarheden en daarop de juiste maatregelen te treffen.		x	

ACTIEPLAN

Domein 1 Handhaving en wijkgericht werken

Legenda voor de beoordeling van de beheersmaatregelen	
Groen	Volledig opgezet, bestaan en/of effectief werken
Geel	Niet volledig opgezet, bestaan en/of effectief werken
Rood	Niet opgezet, bestaan en/of effectief werken
Grijs	Niet van toepassing

Onderwerpen		BIO/Borgingsproduct norm[1]	Externe audit 2022		
			Opzet	Bestaan	Werkin
1. Reikwijdte		P 20.2.3.1 en P 20.2.3.4			
Beheersingsmaatregel	De verwerkingsverantwoordelijke heeft bestanden met politiegegevens binnen de organisatie geïdentificeerd en gedocumenteerd.				
Advies	Zorg voor vastlegging van de periodieke controle op de actualiteit van de vastlegging van bestanden met politiegegevens.				
Actie	1. Maak duidelijk welke gegevens en welke soorten verwerkingen van politiegegevens in Citycontrol en Sharepoint plaatsvinden en of deze verwerkingen enkel binnen die applicaties plaatsvinden. 2. De periodieke controle van verwerkingen van politiegegevens vindt jaarlijks in september/oktober plaats door de hoofden van het verantwoordelijke organisatieonderdeel op initiatief van de Privacy Officer. De Functionaris Gegevensbescherming houdt jaarlijks in oktober/november toezicht op de verwerking van politiegegevens in het kader van de Wpg. De controle en het toezicht vindt door middel van de jaarlijkse interne audit plaats. De privacy officer documenteert deze periodieke controle.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q3 en 4				
2. Doelbinding		P 20.2.3.1			
Beheersingsmaatregel	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.				
Advies	Het register en de doelen van de verwerkingen zijn gedocumenteerd in 'Handboek Wet politiegegevens' in 'BIJLAGE 1: HET REGISTER VAN VERWERKINGEN'. Zorg voor vastlegging van uitgevoerde controles dat bij het verwerken van politiegegevens altijd sprake is van doelbinding en dat de gegevens niet op een onrechtmatige wijze worden verwerkt. Bijvoorbeeld door het beschrijven wanneer en door wie een controle op verschillen in het verwerkingsregister en de huidige situatie heeft plaatsgevonden.				
Actie	3. De periodieke controle van verwerkingen van politiegegevens vindt jaarlijks in september/oktober plaats door de hoofden van het verantwoordelijke organisatieonderdeel op initiatief van de Privacy Officer. De Functionaris Gegevensbescherming houdt jaarlijks in oktober/november toezicht op de verwerking van politiegegevens in het kader van de Wpg. De controle en het toezicht vindt door middel van de jaarlijkse interne audit plaats. De privacy officer documenteert deze periodieke controle.				

[1] Voor de P-verwijzingen naar het Borgingsproduct, zie: https://www.informatiebeveiligingsdienst.nl/product/avg-borgingsproduct-2-0/ (Kolom F in tabblad Controls). Voor de BIO-verwijzingen, zie: https://www.informatiebeveiligingsdienst.nl/product/baseline-informatiebeveiliging-overheid-bio/

Onderwerpen		BIO/Borgingsproduct norm[1]	Externe audit 2022		
			Opzet	Bestaan	Werkin
Voortgang (verwijzing naar document)	Actie 1: Q3 en Q4				
3. Noodzakelijkheid en rechtmatigheid, vermelding herkomst					
Beheersingsmaatregel	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.				
Advies	Zorg voor inhoudelijke controles op noodzakelijkheid en toereikendheid. Leg uitgevoerde controles vast, en op welke dossiers deze controles zijn uitgevoerd.				
Actie	1. Stel een procedure/werkinstructie op waaruit blijkt dat aan de Beheersingsmaatregel wordt voldaan. 2. De periodieke controle van verwerkingen van politiegegevens vindt jaarlijks in september/oktober plaats door de hoofden van het verantwoordelijke organisatieonderdeel op initiatief van de Privacy Officer. De Functionaris Gegevensbescherming houdt jaarlijks in oktober/november toezicht op de verwerking van politiegegevens in het kader van de Wpg. De controle en het toezicht vindt door middel van de jaarlijkse interne audit plaats. De privacy officer documenteert deze periodieke controle.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q3 en Q4				
4. Juistheid en volledigheid politiegegevens		P 20.7.1.3			
Beheersingsmaatregel	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.				
Advies	Richt controles in op kwaliteit ter borging van de juistheid en nauwkeurigheid van politiegegevens. Zorg voor documentatie waaruit blijkt dat dergelijke controles zijn uitgevoerd. Stel een procedure op voor de vernietiging van politiegegevens.				
Actie	1. Stel een procedure/werkinstructie op waaruit blijkt dat aan de Beheersingsmaatregel wordt voldaan en betrek hierbij de gemeentelijke archivaris. 2. Voer een DPIA uit.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q2				
5. Onderscheid feiten en oordeel		Geen overlap			
Beheersingsmaatregel	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.				
Advies	Zorg voor documentatie waaruit blijkt dat een periodieke controle op de uitvoering van de regel dat enkel feiten worden verwerkt heeft plaatsgevonden.				
Actie	1. Maak duidelijk dat bij het verwerken van politiegegevens voldoende inzichtelijk gemaakt is wat een vaststaand feit is, en wat een persoonlijk oordeel, bijvoorbeeld door labeling van de gegevens of een andere werkwijze. 2. De periodieke controle van verwerkingen van politiegegevens vindt jaarlijks in september/oktober plaats door de hoofden van het verantwoordelijke organisatieonderdeel op initiatief van de Privacy Officer. De Functionaris Gegevensbescherming houdt jaarlijks in oktober/november toezicht op de verwerking van politiegegevens in het kader van de Wpg. De controle en het toezicht vindt door middel van de jaarlijkse interne audit plaats. De privacy officer documenteert deze periodieke controle.				
Voortgang (verwijzing naar document)	Actie 1: Q 2 Actie 2: Q3 en 4				
6. Gegevensbescherming door beveiliging en ontwerp (privacy by design)		P 20.6.1.1 P 20.6.1.2 P 20.6.1.3			

Onderwerpen		BIO/Borgingsproduct norm[1]	Externe audit 2022		
			Opzet	Bestaan	Werkin
Beheersingsmaatregel	Er is (aantoonbaar) een risicoanalyse uitgevoerd waaruit het risiconiveau blijkt met betrekking tot ongeoorloofde of onrechtmatige verwerking en tegen opzettelijk verlies, vernietiging of beschadiging. De verwerkingsverantwoordelijke identificeert, evalueert en mitigeert systematisch en periodiek factoren die het beschermen van politiegegevens tegen ongeoorloofde of on rechtmatige 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 (bijvoorbeeld bij ontwikkelingen / wijzigingen).				
Advies	Voer een periodieke risicoanalyse uit en zorg voor een zichtbare relatie tussen de risico's en de genomen of te nemen maatregelen. Evalueer de maatregelen periodiek en leg de evaluatie vast. Zorg voor documentatie waaruit blijkt dat privacy by design is toegepast door de organisatie.				
Actie	1. Voer een DPIA uit. 2. Voer periodieke controle uit op autorisaties en logging v.w.b.t. verlies/vernietiging/beschadiging.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q2				
7. Gegevensbescherming door standaardinstellingen (privacy by default)		P 20.6.1.4 P 20.6.1.5			
Beheersingsmaatregel	De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen om te waarborgen dat standaard: ♦ 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.				
Advies	Zorg voor documentatie waaruit blijkt dat privacy by design/default is toegepast door de organisatie. Zorg voor documentatie waarin is vastgesteld onder welke voorwaarden toegang mag worden verschaft tot politiegegevens. Documenteer hoe is geborgd dat personen toegang hebben tot politiegegevens op basis van doelbinding (bv. periodieke controles).				
Actie	1. Voer een DPIA uit. 2. Autorisatiematrix en periodieke controle op werking. 3. Stel beleid op m.b.t. privacy by design en privacy by default.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q2 Actie 3: Q3				
8. Gegevensbeschermingseffectbeoordeling/ Data protection impact assessment (DPIA)		P 20.2.4.3			
Beheersingsmaatregel	Als een verwerking van persoonsgegevens waarschijnlijk een hoog risico oplevert voor de rechten en vrijheden van betrokkenen, moet een DPIA uitgevoerd worden. De DPIA brengt in kaart welke risico's er bestaan en bevat aanbevelingen voor het wegnemen van die risico's.				
Advies	Zorg voor vastlegging van de herbeoordeling van DPIA's. Voer DPIA's uit.				
Actie	1. Uitvoering van een DPIA waarin vastgelegd wordt wanneer herbeoordeling plaatsvindt. 2. Uitvoeren van de eventuele risicobeperkende maatregelen die daaruit voortvloeien.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q3				
9. Bijzondere categorieën van politiegegevens					
Beheersingsmaatregel	Er vindt geen verwerking van bijzondere categorieën van politiegegevens plaats, tenzij:				

Onderwerpen		BIO/Borgingsproduct norm[1]	Externe audit 2022		
			Opzet	Bestaan	Werkin
	♦ 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.				
Advies	Beschrijf op welke wijze geborgd is dat geen bijzondere categorieën van politiegegevens worden verwerkt. Bijvoorbeeld met steekproeven op dossiers.				
Actie	1. Uitvoeren van een DPIA. 2. Uitvoeren van eventuele risicobeperkende maatregelen die daaruit voortvloeien.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q3				
10. Autorisaties en toegang tot politiegegevens		BIO 9.2.2.1 P 20.6.3.3			
Beheersingsmaatregel	Er is een systeem van autorisaties dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid.				
Advies	Zorg voor een autorisatieprocedure en -matrix waarin het Need to Know principe is opgenomen, en de wijze van uitvoering van de periodieke controle op toegang is opgenomen, en pas deze toe. Zorg voor vastlegging van uitgevoerde controles op toegang tot de systemen. Gebruik voor het opstellen van de autorisatieprocedure het document 'Bijlage 5 Beleid Logische Toegangsbeveiliging (vastgesteld door B en W d.d. 4-4-2018) (1)'.				
Actie	1. Autorisatiematrix opstellen en goedgekeurd door proceseigenaar. 2. Vaststellen van de autorisatieprocedure. 3. Vastlegging van uitgevoerde controles op toegang tot de systemen.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q3 Actie 3: Q3				
11. Autorisaties: aanwijzen functionarissen		Geen overlap			
Beheersingsmaatregel	Er is een actuele lijst van, door de verwerkingsverantwoordelijke aangewezen, bevoegde functionarissen.				
Advies	Documenteer wat er moet gebeuren indien artikel 9 verwerkingen gaan plaatsvinden (bv het aanwijzen van bevoegd functionaris en de bijbehorende extra taken). Neem de beheersingsmaatregel op in 'Handboek Wet politiegegevens'.				
Actie	1. Opstellen van een regeling voor het geval artikel 9 Wpg verwerkingen gaan plaatsvinden.				
Voortgang (verwijzing naar document)	Actie 1: Q2				
12. Onderscheid tussen verschillende categorieën van betrokkenen		Geen overlap			
Beheersingsmaatregel	De verwerkingsverantwoordelijke heeft geborgd dat, voor zover mogelijk, duidelijk onderscheid wordt gemaakt in de verschillende categorieën van betrokkenen.				
Advies	Beschrijf op welke wijze onderscheid wordt gemaakt tussen verdachten, slachtoffers en derden binnen de processen en applicaties, en zorg voor borging daarvan.				
Actie	1. Beschrijving van de wijze van onderscheid tussen betrokkenen binnen de processen en applicaties en opname hiervan in het register van verwerkingen. 2. Borging: jaarlijkse actualisering van het register van verwerkingen.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q3				
13. Verwerker en Verwerkersovereenkomst		BIO 15.1.1.3 P 20.5.1.3			
Beheersingsmaatregel	Bij uitbestedingen van taken moet de verwerker de verwerkingsverantwoordelijke alle informatie ter beschikking stellen om aantoonbaar te maken dat de afspraken in de verwerkersovereenkomst en de Wpg worden nageleefd. Er moeten specifieke afspraken gemaakt worden over de handelswijze bij een inbreuk op de beveiliging.				

Onderwerpen		BIO/Borgingsproduct norm[1]	Externe audit 2022		
			Opzet	Bestaan	Werkin
Advies	Zorg voor een verwerkersovereenkomst met de leverancier van Citycontrol, waarin Wpg eisen zijn meegenomen.				
Actie	1. Opstellen en vaststellen van een verwerkersovereenkomst met Citycontrol die aan de Wpg voldoet.				
Voortgang (verwijzing naar document)	Actie 1: Q2				
14. Geheimhoudingsplicht		BIO 7.3.1.4 BIO 13.2.4.1			
Beheersingsmaatregel	Er is geborgd dat de boa of een andere persoon aan wie politiegegevens ter beschikking zijn gesteld formeel bekend is met de plicht tot geheimhouding en de consequenties bij schending van deze plicht.				
Advies	Zorg voor documentatie waaruit blijkt dat medewerkers de trainingen hebben gevolgd.				
Actie	1. Toon aan dat alle medewerkers een online training moeten doorlopen over privacy en informatiebeveiliging. 2. Zorg voor documentatie waaruit blijkt dat medewerkers de trainingen hebben gevolgd.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q2				
15. Geautomatiseerde individuele besluitvorming		P 20.4.2.3			
Beheersingsmaatregel	Besluiten die uitsluitend zijn gebaseerd op geautomatiseerde verwerking die voor de betrokkene nadelige rechtsgevolgen (kunnen) hebben 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 dat 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.				
Advies	Geen				
Actie	Geen				
Voortgang (verwijzing naar document)	n.v.t.				
16. Uitvoering van de dagelijkse politietaak		BIO 18.1.3.1			
Beheersingsmaatregel	Artikel 8-gegevens (zoals wildplassen, foutief aanbieden van afval, alcoholgebruik op de openbare weg: persoonsgegevens die worden verwerkt in het kader van de dagelijkse opsporingstaak) mogen tot 5 jaar na de eerste verwerkingsdatum met een gerichte zoekvraag worden geraadpleegd of verwerkt.				
Advies	Zorg voor de implementatie van het achter schot plaatsen van politiegegevens in Citycontrol en Sharepoint na 1 jaar, waarna ze enkel nog beschikbaar zijn op hit-no-hit basis.				
Actie	1. Richt Citycontrol en Sharepoint aantoonbaar zo in dat politiegegeven alleen nog maar beschikbaar zijn op grond van een gerichte zoekvraag. 2. Voer een DPIA uit waar deze inrichting een onderdeel van is.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q2				
17. Ter beschikking stellen van politie-gegevens binnen het WPG-domein		P 20.4.6.6			
Beheersingsmaatregel	Verdere verwerking (dus met een ander doel dan het aanvankelijke verwerkingsdoel) van artikel 9-politiegegevens mag alleen na toestemming van de daartoe bevoegde functionaris plaatsvinden.				
Advies	Geen				
Actie	1. Stel een werkwijze op voor het geval van verdere verwerking van artikel 9 gegevens waarin de instemming van de bevoegd functionaris wordt vastgelegd.				

Onderwerpen		BIO/Borgingsproduct norm[1]	Externe audit 2022		
			Opzet	Bestaan	Werkin
Voortgang (verwijzing naar document)	Actie 1: Q2				
18. Geautomatiseerd vergelijken en in combinatie zoeken		P 20.4.2.3			
Beheersingsmaatregel	Politiegegevens kunnen worden vergeleken met andere politiegegevens met als doel om vast te stellen of verbanden bestaan tussen de betreffende gegevens. De verwerkingsmogelijkheden geautomatiseerd vergelijken en in combinatie zoeken zijn gebonden aan strikte criteria (zie artikel 11 Wpg)				
Advies	Geen				
Actie	1. Stel een werkwijze op voor het geval vergelijking met andere politiegegevens met als doel om vast te stellen of verbanden bestaan tussen de betreffende gegevens.				
Voortgang (verwijzing naar document)	Actie 1: Q2				
19. Ondersteunende taken		Geen overlap			
Beheersingsmaatregel	De mogelijkheid bestaat om gegevens die oorspronkelijk zijn verwerkt op basis van artikel 8 of 9 verder te verwerken via een artikel 13-verwerking. Geborgd is dat voor de verwerkingen bedoeld in art 13 lid 1t/m 3, van tevoren is voldaan aan de schriftelijke vereisten (art 13 lid 4). Vooralsnog zijn er geen gevallen bekend van artikel 13-verwerkingen voor Boa's. Er wordt verwacht dat dit in de toekomst wel gaat gebeuren.				
Advies	Geen				
Actie	1. Stel een werkwijze op voor de borging dat voor de verwerkingen bedoeld in art 13 lid 1t/m 3, van tevoren is voldaan aan de schriftelijke vereisten (art 13 lid 4).				
Voortgang (verwijzing naar document)	Actie 1: Q2				
20. Bewaartermijnen, verwijderen en vernietigen		BIO 18.1.3.1			
Beheersingsmaatregel	Politiegegevens mogen niet langer worden bewaard dan is vastgelegd in wet- en regelgeving, of voor de doeleinden waarvoor deze zijn verwerkt. Het is aan de verwerkingsverantwoordelijke om ervoor te zorgen dat de gegevens conform de wet worden gecontroleerd, verwijderd en vernietigd.				
Advies	1. Stel in documentatie vast hoe is geborgd dat politiegegevens worden verwijderd en vernietigd conform de Wet politiegegevens en betrek hierbij de gemeentelijke archivaris. 2. Zorg voor gedocumenteerd bewijs van uitgevoerde verwijderacties.				
Actie	1. Stel een werkwijze op waarin is opgenomen dat politiegegevens worden verwijderd en vernietigd conform de Wpg . Maak daarbij inzichtelijk waar en hoe de gegevens zijn opgeslagen (systemen, archieven, back-ups, overige media), welke typen gegevens vanaf welk moment hoe lang worden bewaard en of en zo ja hoe controlemaatregelen zijn ingericht (geautomatiseerd of handmatig) die ervoor zorgen dat de verschillende typen gegevens op het juiste moment worden verwijderd. 2. Overleg bewijs van uitgevoerde verwijderacties.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q2				
21. Verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee					
Beheersingsmaatregel	Het delen van politiegegevens buiten het Wpg-domein mag alleen onder bepaalde voorwaarden plaatsvinden.				
Advies	Zorg voor documentatie waaruit blijkt dat de beheersmaatregelen in de praktijk zijn toegepast. Beschrijf een procedure voor het in kennis stellen van de ontvanger van politiegegevens indien geconstateerd wordt dat onjuiste politiegegevens zijn verstrekt of dat politiegegevens op onrechtmatig wijze zijn verstrekt. Zorg voor een overzicht van instanties waar verstrekkingen aan plaatsvinden zoals bedoeld in deze beheersmaatregel en artikelen.				

Onderwerpen		BIO/Borgingsproduct norm[1]	Externe audit 2022		
			Opzet	Bestaan	Werkin
Actie	1. Stel vast of het overzicht van instanties waar verstrekkingen aan plaatsvinden volledig is. Ga daarbij onder meer in op bijv. de burgemeester, de Belastingdienst of het CJIB. 2. Stel een werkwijze/procedure op waaruit blijkt dat in geval van verstrekkingen aan de voorwaarden van deze Beheersingsmaatregel wordt voldaan. 3. Als blijkt dat er verstrekkingen plaatsvinden: toon aan dat aan de Beheersingsmaatregel wordt voldaan.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q2 Actie 3: Q3				
22. Doorgiften aan derde landen		P 20.2.6.2			
Beheersingsmaatregel	Het doorgeven van politiegegevens aan derde landen (alle landen buiten de EU, m.u.v. de landen in de EER – Noorwegen, Liechtenstein en IJsland) mag alleen onder bepaalde uitzonderingsgronden.				
Advies	Geen				
Actie	1. Formuleer hoe het eventueel doorgeven aan derde landen wordt getoetst aan de uitzonderingsgronden.				
Voortgang (verwijzing naar document)	Actie 1: Q2				
23. Verstrekking aan derden structureel voor samenwerkingsverbanden		P 20.2.3.1			
Beheersingsmaatregel	Er zijn samenwerkingsverbanden waarbij politiegegevens worden verstrekt (bijvoorbeeld het RIEC). De verwerkingsverantwoordelijke moet vastleggen waarom deze verstrekking plaatsvindt.				
Advies	Stel vast of en documenteer welke samenwerkingsverbanden bestaan waarbij politiegegevens worden verstrekt zoals bedoeld in artikel 20 (betreffende organisaties die niet in het Besluit politiegegevens zijn opgenomen).				
Actie	1. Doe een steekproef om vast te stellen of voldoende is vastgelegd welke gegevensverstrekkingen hebben plaatsgevonden, wat daarvan het doel was, onder welke voorwaarden en aan wie de gegevens verstrekt zijn? 2. Stel vast welke samenwerkingsverbanden bestaan waarbij politiegegevens worden verstrekt zoals bedoeld in artikel 20 Wpg. 3. Stel vast of daarvoor convenanten zijn afgesloten en zo nee stel die vast. 4. Neem deze op in het Handboek Wpg.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q2 Actie 3: Q2 Actie 4: Q3				
24. Rechtstreekse verstrekking		BIO 13.2.1			
Beheersingsmaatregel	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.				
Advies	Geen				
Actie	1. Beschrijf hoe eventuele rechtstreekse verstrekking plaatsvindt en hoe dat is geborgd.				
Voortgang (verwijzing naar document)	Actie 1: Q3				
25. Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering		P 20.4.1.3 P 20.4.3.2			
Beheersingsmaatregel	Verzoeken tot inzage, rectificatie, vernietiging van betrokkenen worden - met inachtneming van het gestelde in artikel 27 - tijdig en adequaat afgehandeld.				

Onderwerpen		BIO/Borgingsproduct norm[1]	Externe audit 2022		
			Opzet	Bestaan	Werkin
Advies	Zorg voor vastlegging waaruit blijkt dat in de loop der jaren de privacyverklaring beschikbaar is op de website en dat uitvoering van de procedure rechten van betrokkenen aantoonbaar is uitgevoerd.				
Actie	Geen (domeinoverstijgend)				
Voortgang (verwijzing naar document)	n.v.t.				
26. Register		P 20.2.3.1			
Beheersingsmaatregel	De verwerkingsverantwoordelijke moet een Register van Verwerkingen bijhouden, waarin een aantal verplichte beschrijvingen moeten zijn opgenomen.				
Advies	Zorg voor consistentie in de bewaartermijnen voor vernietiging en verwijdering, in het document 'Handboek Wet politiegegevens'. Beschrijf bij de verwerkingen de naam en contactgegevens van de verwerkingsverantwoordelijke, de eventuele gezamenlijke verwerkingsverantwoordelijke en de functionaris voor gegevensbescherming. Beschrijf voor alle verwerkingen de rechtsgrondslag en toekenning van autorisaties zoals bedoeld in artikel 6.				
Actie	1. Actualiseer het register van verwerkingen voor alle verplichte onderdelen in het domein.				
Voortgang (verwijzing naar document)	Actie 1: Q2				
27. Documentatie		P 20.2.3.1			
Beheersingsmaatregel	De verwerkingsverantwoordelijke heeft een documentatieplicht. De documentatieplicht heeft niet alleen als doel het afleggen van verantwoording, maar ook het creëren van transparantie rondom de gegevensverwerkingen.				
Advies	Zorg voor invulling en uitvoering van de beheersmaatregelen welke betrekking hebben op artikel 32 lid l t/m 4 van de Wpg. Documenteer welke documentatie moet worden bijgehouden en hoe dat is ingericht binnen de organisatie.				
Actie	1. Inventariseer en documenteer welke documentatie moet worden bijgehouden en hoe dat is ingericht in de organisatie 2. Stel een procedure(s)/werkinstructie(s) voor de documentatieplicht op; 3. Toon aan met steekproeven dat aan de documentatieplicht en bijbehorende eisen wordt voldaan.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q2 Actie 3: Q2				
28. Logging		BIO 12.4.1 BIO 12.4.2 BIO 12.4.3			
Beheersingsmaatregel	De verwerkingsverantwoordelijke en de verwerker dragen zorg voor de logging van verwerkingen zoals opgenomen in art 32a lid l. 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.				
Advies	Zorg voor de inrichting en implementatie van een controleproces voor de periodieke beoordeling van logbestanden van systemen waarin politiegegevens worden verwerkt. Borg de bewaartermijnen van de logging ten behoeve van auditcontroles.				
Actie	1. Zorg ervoor dat het werkproces is ingericht en geïmplementeerd om de logbestanden periodiek te beoordelen. 2. Stel vast voor welke systemen de loggingsplicht van artikel 32a van toepassing is. 3. Toon aan dat conform het logging beleid wordt gewerkt. Ga daarbij in op: - de vraag of loggingbestanden beschikbaar zijn over de afgelopen verslagperiode, waarin in de logregel minimaal het verzamelen, wijzigen, raadplegen, verstrekken (onder meer in de vorm van doorgiften), combineren is vastgelegd. - zijn de logbestanden voldoende beschermd tegen (ongeautoriseerde) wijzigingen?				

Onderwerpen		BIO/Borgingsproduct norm[1]	Externe audit 2022		
			Opzet	Bestaan	Werkin
Voortgang (verwijzing naar document)	Actie 1: Q3 Actie 2: Q3 Actie 3: Q3				
29. Audits		BIO 18.2.1.2			
Beheersingsmaatregel	Er wordt uitvoering gegeven aan de eisen zoals gesteld in de Regeling Periodieke Audit politiegegevens.				
Advies	Zorg voor een vastgestelde auditplanning waaruit blijkt dat uitvoering wordt gegeven aan de eisen zoals gesteld in de Regeling Periodieke Audit politiegegevens (Rpap). Zorg voor de uitvoering van de relevante interne en externe audits conform de Rpap. Beschrijf bijvoorbeeld in het document 'Handboek Wet politiegegevens' ook de planning voor de volgens Rpap vereiste jaarlijkse interne audits.				
Actie	Geen (domeinoverstijgende actie)				
Voortgang (verwijzing naar document)	n.v.t.				
30. Melding datalekken		P 20.6.2.1 P 20.6.2.5			
Beheersingsmaatregel	De organisatie is verplicht om privacy gerelateerde incidenten op gepaste wijze te detecteren en behandelen. Het beperken van de gevolgen en het nemen van maatregelen om toekomstige inbreuken te voorkomen staat hierbij centraal.				
Advies	Geen				
Actie	Geen				
Voortgang (verwijzing naar document)	n.v.t.				
31. Functionaris voor Gegevensbescherming		BIO 18.1.4.1 P 20.7.1.1			
Beheersingsmaatregel	Er moet een functionaris gegevensbescherming (FG) zijn aangesteld die toezicht houdt op het naleven van de Wpg, de uitvoering van DPIA's, de audits, de bewustmaking rondom de verwerking van politiegegevens, het toewijzen van de autorisaties en het beleid van de verwerkingsverantwoordelijke m.b.t. de bescherming van persoonsgegevens.				
Advies	Geen				
Actie	Geen (domeinoverstijgende actiepunten)				
Voortgang (verwijzing naar document)	n.v.t.				

Technische en organisatorische maatregelen		Conclusie		
		Opzet	Bestaan	Werking
1. Wijzigingenbeheer				
Beheersingsmaatregel	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.			
Advies	Zorg voor bewijsvoering waaruit blijkt dat wijzigingenbeheer procesmatig en procedureel wordt uitgevoerd voor Sharepoint door de gemeente Venlo.			
Actie	1. Toon aan dat het wijzigingenbeheer wordt uitgevoerd voor de applicatie die wordt gebruikt.			
Voortgang (verwijzing naar document)	Actie 1: Q3			
2. Logische toegangsbeveiliging				
Beheersingsmaatregel	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			

Technische en organisatorische maatregelen		Conclusie		
		Opzet	Bestaan	Werking
	rechten aan gebruikers, het controleerbaar maken van het gebruik van deze middelen en het automatiseren van arbeidsintensieve taken.			
Advies	Zorg voor een gedocumenteerde autorisatieprocedure voor Sharepoint.			
Actie	1. Stel een autorisatieprocedure voor sharepoint op.			
Voortgang (verwijzing naar document)	Actie 1: Q2			
3. Beheer van kwetsbaarheden (patchmanagement)				
Beheersingsmaatregel	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.			
Advies	Documenteer voor Sharepoint hoe tijdig informatie wordt verkregen over technische kwetsbaarheden en hoe daar op moet worden gereageerd (patchmanagement beleid/procedure).			
Actie	1. Stel een patchmanagement procedure op voor sharepoint.			
Voortgang (verwijzing naar document)	Actie 1: Q2			
4. Cryptografie				
Beheersingsmaatregel	Ter bescherming van politiegegevens behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.			
Advies	Documenteer en implementeer een beleid voor het gebruik van cryptografische beheersmaatregelen.			
Actie	1. Toon aan dat cryptografiebeleid van de gemeente wordt toegepast voor sharepoint.			
Voortgang (verwijzing naar document)	Actie 1: Q3			
5. Vulnerability scans en Penetratietesten				
Beheersingsmaatregel	Penetratietesten en vulnerability scans worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de systemen waarin politiegegevens verwerkt worden.			
Advies	Zorg voor bewijs waaruit blijkt dat penetratietesten en vulnerabilityscans procesmatig en procedureel worden uitgevoerd.			
Actie	1. Vraag op bij de leverancier op welke wijze penetratietesten en vulnerabilityscans worden uitgevoerd.			
Voortgang (verwijzing naar document)	Actie 1: Q2			

Domein 2 Toezicht en handhaving Milieu en bodem

Legenda voor de beoordeling van de beheersmaatregelen	
Groen	Volledig opgezet, bestaan en/of effectief werken
Geel	Niet volledig opgezet, bestaan en/of effectief werken
Rood	Niet opgezet, bestaan en/of effectief werken
Grijs	Niet van toepassing

Onderwerpen		BIO/Borgingsproduct Beheersingsmaatregel[2]	Externe audit 2022		
			Opzet	Bestaan	Werkin
1. Reikwijdte		P 20.2.3.1 en P 20.2.3.4			
Beheersingsmaatregel	De verwerkingsverantwoordelijke heeft bestanden met politiegegevens binnen de organisatie geïdentificeerd en gedocumenteerd.				
Advies	Zorg voor vastlegging van de periodieke controle op de actualiteit van de vastlegging van bestanden met politiegegevens.				
Actie	1. Maak duidelijk welke gegevens en welke soorten verwerkingen van politiegegevens Squit XO plaatsvinden en of deze verwerkingen enkel binnen die applicaties plaatsvinden. 2. De periodieke controle van verwerkingen van politiegegevens vindt jaarlijks in september/oktober plaats door de hoofden van het verantwoordelijke organisatieonderdeel op initiatief van de Privacy Officer. De Functionaris Gegevensbescherming houdt jaarlijks in oktober/november toezicht op de verwerking van politiegegevens in het kader van de Wpg. De controle en het toezicht vindt door middel van de jaarlijkse interne audit plaats. De privacy officer documenteert deze periodieke controle.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q3 en 4				
2. Doelbinding		P 20.2.3.1			
Beheersingsmaatregel	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.				
Advies	Het register en de doelen van de verwerkingen zijn gedocumenteerd in 'Handboek Wet politiegegevens' in 'BIJLAGE 1: HET REGISTER VAN VERWERKINGEN'. Zorg voor vastlegging van uitgevoerde controles dat bij het verwerken van politiegegevens altijd sprake is van doelbinding en dat de gegevens niet op een onrechtmatige wijze worden verwerkt. Bijvoorbeeld door het beschrijven wanneer en door wie een controle op verschillen in het verwerkingsregister en de huidige situatie heeft plaatsgevonden.				
Actie	1. De periodieke controle van verwerkingen van politiegegevens vindt jaarlijks in september/oktober plaats door de hoofden van het verantwoordelijke organisatieonderdeel op initiatief van de Privacy Officer. De Functionaris Gegevensbescherming houdt jaarlijks in oktober/november toezicht op de verwerking van politiegegevens in het kader van de Wpg. De controle en het toezicht vindt door middel van de jaarlijkse interne audit plaats. De privacy officer documenteert deze periodieke controle.				
Voortgang (verwijzing naar document)	Actie 1: Q3 en Q4				
3. Noodzakelijkheid en rechtmatigheid, vermelding herkomst					

[2] Voor de P-verwijzingen naar het Borgingsproduct, zie: https://www.informatiebeveiligingsdienst.nl/product/avg-borgingsproduct-2-0/ (Kolom F in tabblad Controls). Voor de BIO-verwijzingen, zie: https://www.informatiebeveiligingsdienst.nl/product/baseline-informatiebeveiliging-overheid-bio/

Onderwerpen		BIO/Borgingsproduct Beheersingsmaatregel[2]	Externe audit 2022		
			Opzet	Bestaan	Werkin
Beheersingsmaatregel	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.				
Advies	Inhoudelijke controles op noodzakelijkheid en rechtmatigheid op individuele dossiers zijn niet aangetoond. Zorg daarom voor inhoudelijke controles op noodzakelijkheid en toereikendheid. Leg uitgevoerde controles vast, en op welke dossiers deze controles zijn uitgevoerd.				
Actie	1. Stel een procedure/werkinstructie op waaruit blijkt dat aan de Beheersingsmaatregel wordt voldaan. 2. De periodieke controle van verwerkingen van politiegegevens vindt jaarlijks in september/oktober plaats door de hoofden van het verantwoordelijke organisatieonderdeel op initiatief van de Privacy Officer. De Functionaris Gegevensbescherming houdt jaarlijks in oktober/november toezicht op de verwerking van politiegegevens in het kader van de Wpg. De controle en het toezicht vindt door middel van de jaarlijkse interne audit plaats. De privacy officer documenteert deze periodieke controle.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q3 en Q4				
4. Juistheid en volledigheid politiegegevens		P 20.7.1.3			
Beheersingsmaatregel	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.				
Advies	Zorg voor documentatie waaruit blijkt dat dergelijke controles zijn uitgevoerd. Stel een procedure op voor de vernietiging van politiegegevens.				
Actie	1. Stel een procedure/werkinstructie op waaruit blijkt dat aan de Beheersingsmaatregel wordt voldaan en betrek hierbij de gemeentelijke archivaris. 2. Voer een DPIA uit.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q2				
5. Onderscheid feiten en oordeel		Geen overlap			
Beheersingsmaatregel	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.				
Advies	Zorg voor documentatie waaruit blijkt dat een periodieke controle op de uitvoering van de regel dat enkel feiten worden verwerkt heeft plaatsgevonden.				
Actie	1. Maak duidelijk dat bij het verwerken van politiegegevens voldoende inzichtelijk gemaakt is wat een vaststaand feit is, en wat een persoonlijk oordeel, bijvoorbeeld door labeling van de gegevens of een andere werkwijze. 2. De periodieke controle van verwerkingen van politiegegevens vindt jaarlijks in september/oktober plaats door de hoofden van het verantwoordelijke organisatieonderdeel op initiatief van de Privacy Officer. De Functionaris Gegevensbescherming houdt jaarlijks in oktober/november toezicht op de verwerking van politiegegevens in het kader van de Wpg. De controle en het toezicht vindt door middel van de jaarlijkse interne audit plaats. De privacy officer documenteert deze periodieke controle.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q3 en 4				
6. Gegevensbescherming door beveiliging en ontwerp (privacy by design)		P 20.6.1.1 P 20.6.1.2 P 20.6.1.3			
Beheersingsmaatregel	Er is (aantoonbaar) een risicoanalyse uitgevoerd waaruit het risiconiveau blijkt met betrekking tot ongeoorloofde of onrechtmatige verwerking en tegen opzettelijk verlies, vernietiging of beschadiging.				

Onderwerpen		BIO/Borgingsproduct Beheersingsmaatregel[2]	Externe audit 2022		
			Opzet	Bestaan	Werkin
	De verwerkingsverantwoordelijke identificeert, evalueert en mitigeert systematisch en periodiek factoren die het beschermen van politiegegevens tegen ongeoorloofde of on rechtmatige 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 (bijvoorbeeld bij ontwikkelingen / wijzigingen).			
Advies	Voer een periodieke risicoanalyse uit en zorg voor een zichtbare relatie tussen de risico's en de genomen of te nemen maatregelen. Evalueer de maatregelen periodiek en leg de evaluatie vast. Zorg voor documentatie waaruit blijkt dat privacy by design is toegepast door de organisatie.				
Actie	1. Voer een DPIA uit. 2. Voer periodieke controle uit op autorisaties en logging v.w.b.t. verlies/vernietiging/beschadiging.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q2				
7. Gegevensbescherming door standaardinstellingen (privacy by default)		P 20.6.1.4 P 20.6.1.5			
Beheersingsmaatregel	De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen om te waarborgen dat standaard: ♦ 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.				
Advies	Zorg voor documentatie waaruit blijkt dat privacy by design/default is toegepast door de organisatie. Zorg voor documentatie waarin is vastgesteld onder welke voorwaarden toegang mag worden verschaft tot politiegegevens. Documenteer hoe is geborgd dat personen toegang hebben tot politiegegevens op basis van doelbinding (bv. periodieke controles).				
Actie	1. Voer een DPIA uit. 2. Nog in te vullen. 3. Stel beleid op m.b.t. privacy by design en privacy by default.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q2 Actie 3: Q3				
8. Gegevensbeschermingseffectbeoordeling/ Data protection impact assessment (DPIA)		P 20.2.4.3			
Beheersingsmaatregel	Als een verwerking van persoonsgegevens waarschijnlijk een hoog risico oplevert voor de rechten en vrijheden van betrokkenen, moet een DPIA uitgevoerd worden. De DPIA brengt in kaart welke risico's er bestaan en bevat aanbevelingen voor het wegnemen van die risico's.				
Advies	Zorg voor vastlegging van de herbeoordeling van DPIA's. Voer DPIA's uit.				
Actie	1. Uitvoering van een DPIA. 2. Uitvoeren van de eventuele risicobeperkende maatregelen die daaruit voortvloeien.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q3				
9. Bijzondere categorieën van politiegegevens					
Beheersingsmaatregel	Er vindt geen verwerking van bijzondere categorieën van politiegegevens plaats, tenzij: ♦ 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.				

Onderwerpen		BIO/Borgingsproduct Beheersingsmaatregel[2]	Externe audit 2022		
			Opzet	Bestaan	Werkin
Advies	Beschrijf op welke wijze geborgd is dat geen bijzondere categorieën van politiegegevens worden verwerkt. Bijvoorbeeld met steekproeven op dossiers.				
Actie	1. Uitvoeren van een DPIA. 2. Uitvoeren van eventuele risicobeperkende maatregelen die daaruit voortvloeien.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q3				
10. Autorisaties en toegang tot politiegegevens		BIO 9.2.2.1 P 20.6.3.3			
Beheersingsmaatregel	Er is een systeem van autorisaties dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid.				
Advies	Zorg voor een autorisatieprocedure en -matrix waarin het Need to Know principe is opgenomen, en de wijze van uitvoering van de periodieke controle op toegang is opgenomen, en pas deze toe. Zorg voor vastlegging van uitgevoerde controles op toegang tot de systemen. Gebruik voor het opstellen van de autorisatieprocedure het document 'Bijlage 5 Beleid Logische Toegangsbeveiliging (vastgesteld door B en W d.d. 4-4-2018) (1)'.				
Actie	1. Autorisatiematrix opstellen en goedgekeurd door proceseigenaar. 2. Vaststellen van de autorisatieprocedure. 3. Vastlegging van uitgevoerde controles op toegang tot de systemen.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q3 Actie 3: Q3				
11. Autorisaties: aanwijzen functionarissen		Geen overlap			
Beheersingsmaatregel	Er is een actuele lijst van, door de verwerkingsverantwoordelijke aangewezen, bevoegde functionarissen.				
Advies	Documenteer wat er moet gebeuren indien artikel 9 verwerkingen gaan plaatsvinden (bv het aanwijzen van bevoegd functionaris en de bijbehorende extra taken). Neem de beheersingsmaatregel op in 'Handboek Wet politiegegevens'.				
Actie	1. Opstellen van een regeling voor het geval artikel 9 Wpg verwerkingen gaan plaatsvinden.				
Voortgang (verwijzing naar document)	Actie 1: Q2				
12. Onderscheid tussen verschillende categorieën van betrokkenen		Geen overlap			
Beheersingsmaatregel	De verwerkingsverantwoordelijke heeft geborgd dat, voor zover mogelijk, duidelijk onderscheid wordt gemaakt in de verschillende categorieën van betrokkenen.				
Advies	Beschrijf op welke wijze onderscheid wordt gemaakt tussen verdachten, slachtoffers en derden binnen de processen en applicaties, en zorg voor borging daarvan.				
Actie	1. Beschrijving van de wijze van onderscheid tussen betrokkenen binnen de processen en applicaties. 2. Borging: jaarlijkse actualisering van het register van verwerkingen.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q3				
13. Verwerker en Verwerkersovereenkomst		BIO 15.1.1.3 P 20.5.1.3			
Beheersingsmaatregel	Bij uitbestedingen van taken moet de verwerker de verwerkingsverantwoordelijke alle informatie ter beschikking stellen om aantoonbaar te maken dat de afspraken in de verwerkersovereenkomst en de Wpg worden nageleefd. Er moeten specifieke afspraken gemaakt worden over de handelswijze bij een inbreuk op de beveiliging.				
Advies	Zorg voor een verwerkersovereenkomst met de leverancier van SquitXO, waarin Wpg eisen zijn meegenomen.				
Actie	1. Opstellen en vaststellen van een verwerkersovereenkomst met Visma Roxit NL die aan de Wpg voldoet.				

Onderwerpen		BIO/Borgingsproduct Beheersingsmaatregel[2]	Externe audit 2022		
			Opzet	Bestaan	Werkin
Voortgang (verwijzing naar document)	Actie 1: Q2				
14. Geheimhoudingsplicht		BIO 7.3.1.4 BIO 13.2.4.1			
Beheersingsmaatregel	Er is geborgd dat de boa of een andere persoon aan wie politiegegevens ter beschikking zijn gesteld formeel bekend is met de plicht tot geheimhouding en de consequenties bij schending van deze plicht.				
Advies	Zorg voor documentatie waaruit blijkt dat medewerkers de trainingen hebben gevolgd.				
Actie	1. Toon aan dat alle medewerkers een online training moeten doorlopen over privacy en informatiebeveiliging. 2. Zorg voor documentatie waaruit blijkt dat medewerkers de trainingen hebben gevolgd.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q2				
15. Geautomatiseerde individuele besluitvorming		P 20.4.2.3			
Beheersingsmaatregel	Besluiten die uitsluitend zijn gebaseerd op geautomatiseerde verwerking die voor de betrokkene nadelige rechtsgevolgen (kunnen) hebben 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 dat 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.				
Advies	Geen				
Actie	Geen				
Voortgang (verwijzing naar document)	n.v.t.				
16. Uitvoering van de dagelijkse politietaak		BIO 18.1.3.1			
Beheersingsmaatregel	Artikel 8-gegevens (zoals wildplassen, foutief aanbieden van afval, alcoholgebruik op de openbare weg: persoonsgegevens die worden verwerkt in het kader van de dagelijkse opsporingstaak) mogen tot 5 jaar na de eerste verwerkingsdatum met een gerichte zoekvraag worden geraadpleegd of verwerkt.				
Advies	Zorg voor de implementatie van het achter schot plaatsen van politiegegevens in SquitXO en Sharepoint na 1 jaar, waarna ze enkel nog beschikbaar zijn op hit-no-hit basis.				
Actie	1. Richt SquitXO en Sharepoint aantoonbaar zo in dat politiegegeven alleen nog maar beschikbaar zijn op grond van een gerichte zoekvraag. 2. Voer een DPIA uit waar deze inrichting een onderdeel van is.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q2				
17. Ter beschikking stellen van politie-gegevens binnen het WPG-domein		P 20.4.6.6			
Beheersingsmaatregel	Verdere verwerking (dus met een ander doel dan het aanvankelijke verwerkingsdoel) van artikel 9-politiegegevens mag alleen na toestemming van de daartoe bevoegde functionaris plaatsvinden.				
Advies	Geen				
Actie	1. Stel een werkwijze op voor het geval van verdere verwerking van artikel 9 gegevens waarin de instemming van de bevoegd functionaris wordt vastgelegd.				
Voortgang (verwijzing naar document)	Actie 1: Q2				
18. Geautomatiseerd vergelijken en in combinatie zoeken		P 20.4.2.3			

Onderwerpen		BIO/Borgingsproduct Beheersingsmaatregel[2]	Externe audit 2022		
			Opzet	Bestaan	Werkin
Beheersingsmaatregel	Politiegegevens kunnen worden vergeleken met andere politiegegevens met als doel om vast te stellen of verbanden bestaan tussen de betreffende gegevens. De verwerkingsmogelijkheden geautomatiseerd vergelijken en in combinatie zoeken zijn gebonden aan strikte criteria (zie artikel 11 Wpg)				
Advies	Geen				
Actie	1. Stel een werkwijze op voor het geval vergelijking met andere politiegegevens met als doel om vast te stellen of verbanden bestaan tussen de betreffende gegevens. 2. Neem deze werkwijze op in het Handboek Wpg.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q3				
19. Ondersteunende taken		Geen overlap			
Beheersingsmaatregel	De mogelijkheid bestaat om gegevens die oorspronkelijk zijn verwerkt op basis van artikel 8 of 9 verder te verwerken via een artikel 13-verwerking. Geborgd is dat voor de verwerkingen bedoeld in art 13 lid 1t/m 3, van tevoren is voldaan aan de schriftelijke vereisten (art 13 lid 4). Vooralsnog zijn er geen gevallen bekend van artikel 13-verwerkingen voor Boa's. Er wordt verwacht dat dit in de toekomst wel gaat gebeuren.				
Advies	Geen				
Actie	1. Stel een werkwijze op voor de borging dat voor de verwerkingen bedoeld in art 13 lid 1t/m 3, van tevoren is voldaan aan de schriftelijke vereisten (art 13 lid 4).				
Voortgang (verwijzing naar document)	Actie 1: Q2				
20. Bewaartermijnen, verwijderen en vernietigen		BIO 18.1.3.1			
Beheersingsmaatregel	Politiegegevens mogen niet langer worden bewaard dan is vastgelegd in wet- en regelgeving, of voor de doeleinden waarvoor deze zijn verwerkt. Het is aan de verwerkingsverantwoordelijke om ervoor te zorgen dat de gegevens conform de wet worden gecontroleerd, verwijderd en vernietigd.				
Advies	Stel in documentatie vast hoe is geborgd dat politiegegevens worden verwijderd en vernietigd conform de Wet politiegegevens. Zorg voor gedocumenteerd bewijs van uitgevoerde verwijderacties.				
Actie	1. Stel een werkwijze op waarin is opgenomen dat politiegegevens worden verwijderd en vernietigd conform de Wpg . Maak daarbij inzichtelijk waar en hoe de gegevens zijn opgeslagen (systemen, archieven, back-ups, overige media), welke typen gegevens vanaf welk moment hoe lang worden bewaard en of en zo ja hoe controlemaatregelen zijn ingericht (geautomatiseerd of handmatig) die ervoor zorgen dat de verschillende typen gegevens op het juiste moment worden verwijderd. 2. Overleg bewijs van uitgevoerde verwijderacties.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q2				
21. Verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee					
Beheersingsmaatregel	Het delen van politiegegevens buiten het Wpg-domein mag alleen onder bepaalde voorwaarden plaatsvinden.				
Advies	Zorg voor documentatie waaruit blijkt dat de beheersmaatregelen in de praktijk zijn toegepast. Beschrijf een procedure voor het in kennis stellen van de ontvanger van politiegegevens indien geconstateerd wordt dat onjuiste politiegegevens zijn verstrekt of dat politiegegevens op onrechtmatig wijze zijn verstrekt. Zorg voor een overzicht van instanties waar verstrekkingen aan plaatsvinden zoals bedoeld in deze beheersmaatregel en artikelen.				
Actie	1. Stel vast of het overzicht van instanties waar verstrekkingen aan plaatsvinden volledig is. Ga daarbij onder meer in op bijv. de burgemeester, de Belastingdienst of het CJIB. 2. Stel een werkwijze/procedure op waaruit blijkt dat in geval van verstrekkingen aan de voorwaarden van deze Beheersingsmaatregel wordt voldaan.				

Onderwerpen		BIO/Borgingsproduct Beheersingsmaatregel[2]	Externe audit 2022		
			Opzet	Bestaan	Werkin
	3. Als blijkt dat er verstrekkingen plaatsvinden: toon aan dat aan de Beheersingsmaatregel wordt voldaan.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q2 Actie 3: Q3				
22. Doorgiften aan derde landen		P 20.2.6.2			
Beheersingsmaatregel	**Het doorgeven van politiegegevens aan derde landen (alle landen buiten de EU, m.u.v. de landen in de EER – Noorwegen, Liechtenstein en IJsland) mag alleen onder bepaalde uitzonderingsgronden.**				
Advies	Geen				
Actie	1. Formuleer hoe het eventueel doorgeven aan derde landen wordt getoetst aan de uitzonderingsgronden.				
Voortgang (verwijzing naar document)	**Actie 1: Q2**				
23. Verstrekking aan derden structureel voor samenwerkingsverbanden		P 20.2.3.1			
Beheersingsmaatregel	Er zijn samenwerkingsverbanden waarbij politiegegevens worden verstrekt (bijvoorbeeld het RIEC). De verwerkingsverantwoordelijke moet vastleggen waarom deze verstrekking plaatsvindt.				
Advies	Stel vast of en documenteer welke samenwerkingsverbanden bestaan waarbij politiegegevens worden verstrekt zoals bedoeld in artikel 20 (betreffende organisaties die niet in het Besluit politiegegevens zijn opgenomen).				
Actie	1. Doe een steekproef om vast te stellen of voldoende is vastgelegd welke gegevensverstrekkingen hebben plaatsgevonden, wat daarvan het doel was, onder welke voorwaarden en aan wie de gegevens verstrekt zijn? 2. Stel vast welke samenwerkingsverbanden bestaan waarbij politiegegevens worden verstrekt zoals bedoeld in artikel 20 Wpg 3. Stel vast of daarvoor convenanten zijn afgesloten en zo nee stel die vast; 4. Neem deze op in het Handboek Wpg				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q2 Actie 3: Q2 Actie 4: Q3				
24. Rechtstreekse verstrekking		BIO 13.2.1			
Beheersingsmaatregel	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				
Advies	Geen				
Actie	1. Beschrijf hoe eventuele rechtstreekse verstrekking plaatsvindt en hoe dat is geborgd.				
Voortgang (verwijzing naar document)	Actie 1: Q3				
25. Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering		P 20.4.1.3 P 20.4.3.2			
Beheersingsmaatregel	Verzoeken tot inzage, rectificatie, vernietiging van betrokkenen worden - met inachtneming van het gestelde in artikel 27 - tijdig en adequaat afgehandeld.				
Advies	Zorg voor vastlegging waaruit blijkt dat in de loop der jaren de privacyverklaring beschikbaar is op de website en dat uitvoering van de procedure rechten van betrokkenen aantoonbaar is uitgevoerd.				
Actie	Geen (domeinoverstijgend)				
Voortgang (verwijzing naar document)	n.v.t.				

Onderwerpen		BIO/Borgingsproduct Beheersingsmaatregel[2]	Externe audit 2022		
			Opzet	Bestaan	Werkin
26. Register		P 20.2.3.1			
Beheersingsmaatregel	De verwerkingsverantwoordelijke moet een Register van Verwerkingen bijhouden, waarin een aantal verplichte beschrijvingen moeten zijn opgenomen.				
Advies	Zorg voor consistentie in de bewaartermijnen voor vernietiging en verwijdering, in het document 'Handboek Wet politiegegevens'. Beschrijf bij de verwerkingen de naam en contactgegevens van de verwerkingsverantwoordelijke, de eventuele gezamenlijke verwerkingsverantwoordelijke en de functionaris voor gegevensbescherming. Beschrijf voor alle verwerkingen de rechtsgrondslag en toekenning van autorisaties zoals bedoeld in artikel 6.				
Actie	1. Actualiseer het register van verwerkingen voor alle verplichte onderdelen in het domein				
Voortgang (verwijzing naar document)	Actie 1: Q3				
27. Documentatie		P 20.2.3.1			
Beheersingsmaatregel	De verwerkingsverantwoordelijke heeft een documentatieplicht. De documentatieplicht heeft niet alleen als doel het afleggen van verantwoording, maar ook het creëren van transparantie rondom de gegevensverwerkingen.				
Advies	Zorg voor invulling en uitvoering van de beheersmaatregelen welke betrekking hebben op artikel 32 lid l t/m 4 van de Wpg. Documenteer welke documentatie moet worden bijgehouden en hoe dat is ingericht binnen de organisatie.				
Actie	1. Inventariseer en documenteer welke documentatie moet worden bijgehouden en hoe dat is ingericht in de organisatie. 2. Stel een procedure(s)/werkinstructie(s) voor de documentatieplicht op. 3. Toon aan met steekproeven dat aan de documentatieplicht en bijbehorende eisen wordt voldaan.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q2 Actie 3: Q2				
28. Logging		BIO 12.4.1 BIO 12.4.2 BIO 12.4.3			
Beheersingsmaatregel	De verwerkingsverantwoordelijke en de verwerker dragen zorg voor de logging van verwerkingen zoals opgenomen in art 32a lid l. 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.				
Advies	Zorg voor de inrichting en implementatie van een controleproces voor de periodieke beoordeling van logbestanden van systemen waarin politiegegevens worden verwerkt. Borg de bewaartermijnen van de logging ten behoeve van auditcontroles.				
Actie	1. Zorg ervoor dat het werkproces is ingericht en geïmplementeerd om de logbestanden periodiek te beoordelen. 2. Stel vast voor welke systemen de loggingsplicht van artikel 32a van toepassing is. 3. Toon aan dat conform het logging beleid wordt gewerkt. Ga daarbij in op: - de vraag of loggingbestanden beschikbaar zijn over de afgelopen verslagperiode, waarin in de logregel minimaal het verzamelen, wijzigen, raadplegen, verstrekken (onder meer in de vorm van doorgiften), combineren is vastgelegd. - zijn de logbestanden voldoende beschermd tegen (ongeautoriseerde) wijzigingen?				
Voortgang (verwijzing naar document)	Actie 1: Q3 Actie 2: Q3 Actie 3: Q3				
29. Audits		BIO 18.2.1.2			
Beheersingsmaatregel	Er wordt uitvoering gegeven aan de eisen zoals gesteld in de Regeling Periodieke Audit politiegegevens.				

Onderwerpen		BIO/Borgingsproduct Beheersingsmaatregel[2]	Externe audit 2022		
			Opzet	Bestaan	Werkin
Advies	Zorg voor een vastgestelde auditplanning waaruit blijkt dat uitvoering wordt gegeven aan de eisen zoals gesteld in de Regeling Periodieke Audit politiegegevens (Rpap). Zorg voor de uitvoering van de relevante interne en externe audits conform de Rpap. Beschrijf bijvoorbeeld in het document 'Handboek Wet politiegegevens' ook de planning voor de volgens Rpap vereiste jaarlijkse interne audits.				
Actie	Geen (domeinoverstijgende actie)				
Voortgang (verwijzing naar document)	n.v.t.				
30. Melding datalekken		P 20.6.2.1 P 20.6.2.5			
Beheersingsmaatregel	De organisatie is verplicht om privacygerelateerde incidenten op gepaste wijze te detecteren en behandelen. Het beperken van de gevolgen en het nemen van maatregelen om toekomstige inbreuken te voorkomen staat hierbij centraal.				
Advies	Geen				
Actie	Geen				
Voortgang (verwijzing naar document)	n.v.t.				
31. Functionaris voor Gegevensbescherming		BIO 18.1.4.1 P 20.7.1.1			
Beheersingsmaatregel	Er moet een functionaris gegevensbescherming (FG) zijn aangesteld die toezicht houdt op het naleven van de Wpg, de uitvoering van DPIA's, de audits, de bewustmaking rondom de verwerking van politiegegevens, het toewijzen van de autorisaties en het beleid van de verwerkingsverantwoordelijke m.b.t. de bescherming van persoonsgegevens.				
Advies	Geen				
Actie	Geen (domeinoverstijgende actiepunten)				
Voortgang (verwijzing naar document)	n.v.t.				

Technische en organisatorische maatregelen		Conclusie		
		Opzet	Bestaan	Werking
1. Wijzigingenbeheer				
Beheersingsmaatregel	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.			
Advies	Zorg voor bewijsvoering waaruit blijkt dat wijzigingenbeheer procesmatig en procedureel wordt uitgevoerd door de gemeente Venlo			
Actie	1. Toon aan dat het wijzigingenbeheer wordt uitgevoerd voor de applicatie die wordt gebruikt.			
Voortgang (verwijzing naar document)	Actie 1: Q3			
2. Logische toegangsbeveiliging				
Beheersingsmaatregel	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.			
Advies	Zorg voor een gedocumenteerde autorisatieprocedure voor Squit XO.			
Actie	1. Stel een autorisatieprocedure op voor de applicatie die wordt gebruikt			

Technische en organisatorische maatregelen		Conclusie		
		Opzet	Bestaan	Werking
Voortgang (verwijzing naar document)	Actie 1: Q3			
3. Beheer van kwetsbaarheden (patchmanagement)				
Beheersingsmaatregel	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.			
Advies	Documenteer voor Squit XO hoe tijdig informatie wordt verkregen over technische kwetsbaarheden en hoe daar op moet worden gereageerd (patchmanagement beleid/procedure).			
Actie	1. Stel een patchmanagement procedure op voor de applicatie die wordt gebruikt.			
Voortgang (verwijzing naar document)	Actie 1: Q3			
4. Cryptografie				
Beheersingsmaatregel	Ter bescherming van politiegegevens behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.			
Advies	Documenteer en implementeer een beleid voor het gebruik van cryptografische beheersmaatregelen.			
Actie	1. Toon aan dat cryptografiebeleid van de gemeente wordt toegepast voor de applicatie die wordt gebruikt.			
Voortgang (verwijzing naar document)	Actie 1: Q3			
5. Vulnerability scans en Penetratietesten				
Beheersingsmaatregel	Penetratietesten en vulnerability scans worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de systemen waarin politiegegevens verwerkt worden.			
Advies	Zorg voor bewijs waaruit blijkt dat penetratietesten en vulnerabilityscans procesmatig en procedureel worden uitgevoerd.			
Actie	1. Vraag op bij de leverancier op welke wijze penetratietesten en vulnerabilityscans worden uitgevoerd.			
Voortgang (verwijzing naar document)	Actie 1: Q2			

Domein 3 Leerplicht RMC Werk

Legenda voor de beoordeling van de beheersmaatregelen	
Groen	Volledig opgezet, bestaan en/of effectief werken
Geel	Niet volledig opgezet, bestaan en/of effectief werken
Rood	Niet opgezet, bestaan en/of effectief werken
Grijs	Niet van toepassing

Onderwerpen		BIO/Borgingsproduct Beheersingsmaatregel[3]	Externe audit 2022		
			Opzet	Bestaan	Werkin
1. Reikwijdte		P 20.2.3.1 en P 20.2.3.4			
Beheersingsmaatregel	De verwerkingsverantwoordelijke heeft bestanden met politiegegevens binnen de organisatie geïdentificeerd en gedocumenteerd.				
Advies	Zorg voor vastlegging van de periodieke controle op de actualiteit van de vastlegging van bestanden met politiegegevens.				
Actie	1. Maak duidelijk welke gegevens en welke soorten verwerkingen van politiegegevens in Carel en zaaksysteem plaatsvinden en of deze verwerkingen enkel binnen die applicaties plaatsvinden. 2. De periodieke controle van verwerkingen van politiegegevens vindt jaarlijks in september/oktober plaats door de hoofden van het verantwoordelijke organisatieonderdeel op initiatief van de Privacy Officer. De Functionaris Gegevensbescherming houdt jaarlijks in oktober/november toezicht op de verwerking van politiegegevens in het kader van de Wpg. De controle en het toezicht vindt door middel van de jaarlijkse interne audit plaats. De privacy officer documenteert deze periodieke controle.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q3 en 4				
2. Doelbinding		P 20.2.3.1			
Beheersingsmaatregel	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.				
Advies	Het register en de doelen van de verwerkingen zijn gedocumenteerd in 'Handboek Wet politiegegevens' in 'BIJLAGE 1: HET REGISTER VAN VERWERKINGEN'. Zorg voor vastlegging van uitgevoerde controles dat bij het verwerken van politiegegevens altijd sprake is van doelbinding en dat de gegevens niet op een onrechtmatige wijze worden verwerkt. Bijvoorbeeld door het beschrijven wanneer en door wie een controle op verschillen in het verwerkingsregister en de huidige situatie heeft plaatsgevonden.				
Actie	1. De periodieke controle van verwerkingen van politiegegevens vindt jaarlijks in september/oktober plaats door de hoofden van het verantwoordelijke organisatieonderdeel op initiatief van de Privacy Officer. De Functionaris Gegevensbescherming houdt jaarlijks in oktober/november toezicht op de verwerking van politiegegevens in het kader van de Wpg. De controle en het toezicht vindt door middel van de jaarlijkse interne audit plaats. De privacy officer documenteert deze periodieke controle.				
Voortgang (verwijzing naar document)	Actie 1: Q3 en Q4				
3. Noodzakelijkheid en rechtmatigheid, vermelding herkomst					

[3] Voor de P-verwijzingen naar het Borgingsproduct, zie: https://www.informatiebeveiligingsdienst.nl/product/avg-borgingsproduct-2-0/ (Kolom F in tabblad Controls). Voor de BIO-verwijzingen, zie: https://www.informatiebeveiligingsdienst.nl/product/baseline-informatiebeveiliging-overheid-bio/

Onderwerpen		BIO/Borgingsproduct Beheersingsmaatregel[3]	Externe audit 2022		
			Opzet	Bestaan	Werkin
Beheersingsmaatregel	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.				
Advies	Zorg voor inhoudelijke controles op noodzakelijkheid en toereikendheid. Leg uitgevoerde controles vast, en op welke dossiers deze controles zijn uitgevoerd.				
Actie	1. Stel een procedure/werkinstructie op waaruit blijkt dat aan de Beheersingsmaatregel wordt voldaan. 2. De periodieke controle van verwerkingen van politiegegevens vindt jaarlijks in september/oktober plaats door de hoofden van het verantwoordelijke organisatieonderdeel op initiatief van de Privacy Officer. De Functionaris Gegevensbescherming houdt jaarlijks in oktober/november toezicht op de verwerking van politiegegevens in het kader van de Wpg. De controle en het toezicht vindt door middel van de jaarlijkse interne audit plaats. De privacy officer documenteert deze periodieke controle.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q3 en Q4				
4. Juistheid en volledigheid politiegegevens		P 20.7.1.3			
Beheersingsmaatregel	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.				
Advies	Richt controles in op kwaliteit ter borging van de juistheid en nauwkeurigheid van politiegegevens. Zorg voor documentatie waaruit blijkt dat dergelijke controles zijn uitgevoerd. Stel een procedure op voor de vernietiging van politiegegevens.				
Actie	1. Stel een procedure/werkinstructie op waaruit blijkt dat aan de Beheersingsmaatregel wordt voldaan en betrek hierbij de gemeentelijke archivaris. 2. Voer een DPIA uit.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q2				
5. Onderscheid feiten en oordeel		Geen overlap			
Beheersingsmaatregel	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.				
Advies	Zorg voor documentatie waaruit blijkt dat een periodieke controle op de uitvoering van de regel dat enkel feiten worden verwerkt heeft plaatsgevonden.				
Actie	1. Maak duidelijk dat bij het verwerken van politiegegevens voldoende inzichtelijk gemaakt is wat een vaststaand feit is, en wat een persoonlijk oordeel, bijvoorbeeld door labeling van de gegevens of een andere werkwijze. 2. De periodieke controle van verwerkingen van politiegegevens vindt jaarlijks in september/oktober plaats door de hoofden van het verantwoordelijke organisatieonderdeel op initiatief van de Privacy Officer. De Functionaris Gegevensbescherming houdt jaarlijks in oktober/november toezicht op de verwerking van politiegegevens in het kader van de Wpg. De controle en het toezicht vindt door middel van de jaarlijkse interne audit plaats. De privacy officer documenteert deze periodieke controle.				
Voortgang (verwijzing naar document)	Actie 1: Q 2 Actie 2: Q3 en 4				
6. Gegevensbescherming door beveiliging en ontwerp (privacy by design)		P 20.6.1.1 P 20.6.1.2 P 20.6.1.3			
Beheersingsmaatregel	Er is (aantoonbaar) een risicoanalyse uitgevoerd waaruit het risiconiveau blijkt met betrekking tot ongeoorloofde of onrechtmatige verwerking en tegen opzettelijk verlies, vernietiging of beschadiging.				

Onderwerpen		BIO/Borgingsproduct Beheersingsmaatregel[3]	Externe audit 2022		
			Opzet	Bestaan	Werkin
	De verwerkingsverantwoordelijke identificeert, evalueert en mitigeert systematisch en periodiek factoren die het beschermen van politiegegevens tegen ongeoorloofde of on rechtmatige 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 (bijvoorbeeld bij ontwikkelingen / wijzigingen).			
Advies	Voer een periodieke risicoanalyse uit en zorg voor een zichtbare relatie tussen de risico's en de genomen of te nemen maatregelen. Evalueer de maatregelen periodiek en leg de evaluatie vast. Zorg voor documentatie waaruit blijkt dat privacy by design is toegepast door de organisatie.				
Actie	1. Voer een DPIA uit. 2. Voer periodieke controle uit op autorisaties en logging v.w.b.t. verlies/ vernietiging/beschadiging.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q2				
7. Gegevensbescherming door standaardinstellingen (privacy by default)		P 20.6.1.4 P 20.6.1.5			
Beheersingsmaatregel	De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen om te waarborgen dat standaard: ♦ 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.				
Advies	Zorg voor documentatie waaruit blijkt dat privacy by design/default is toegepast door de organisatie. Zorg voor documentatie waarin is vastgesteld onder welke voorwaarden toegang mag worden verschaft tot politiegegevens. Documenteer hoe is geborgd dat personen toegang hebben tot politiegegevens op basis van doelbinding (bv. periodieke controles).				
Actie	1. Voer een DPIA uit.				
Voortgang (verwijzing naar document)	Actie 1: Q2				
8. Gegevensbeschermingseffectbeoordeling/ Data protection impact assessment (DPIA)		P 20.2.4.3			
Beheersingsmaatregel	Als een verwerking van persoonsgegevens waarschijnlijk een hoog risico oplevert voor de rechten en vrijheden van betrokkenen, moet een DPIA uitgevoerd worden. De DPIA brengt in kaart welke risico's er bestaan en bevat aanbevelingen voor het wegnemen van die risico's.				
Advies	Zorg voor vastlegging van de herbeoordeling van DPIA's. Voer DPIA's uit.				
Actie	1. Uitvoering van een DPIA. 2. Uitvoeren van de eventuele risicobeperkende maatregelen die daaruit voortvloeien.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q3				
9. Bijzondere categorieën van politiegegevens					
Beheersingsmaatregel	Er vindt geen verwerking van bijzondere categorieën van politiegegevens plaats, tenzij: ♦ 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.				
Advies	Beschrijf op welke wijze geborgd is dat geen bijzondere categorieën van politiegegevens worden verwerkt. Bijvoorbeeld met steekproeven op dossiers.				
Actie	1. Uitvoeren van een DPIA.				

Onderwerpen		BIO/Borgingsproduct Beheersingsmaatregel[3]	Externe audit 2022		
			Opzet	Bestaan	Werkin
	2. Uitvoeren van eventuele risicobeperkende maatregelen die daaruit voortvloeien.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q3				
10. Autorisaties en toegang tot politiegegevens		BIO 9.2.2.1 P 20.6.3.3			
Beheersingsmaatregel	Er is een systeem van autorisaties dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid.				
Advies	Zorg voor een autorisatieprocedure en -matrix waarin het Need to Know principe is opgenomen, en de wijze van uitvoering van de periodieke controle op toegang is opgenomen, en pas deze toe. Zorg voor vastlegging van uitgevoerde controles op toegang tot de systemen. Gebruik voor het opstellen van de autorisatieprocedure het document 'Bijlage 5 Beleid Logische Toegangsbeveiliging (vastgesteld door B en W d.d. 4-4-2018) (1)'.				
Actie	1. Autorisatiematrix opstellen en goedgekeurd door proceseigenaar. 2. Vaststellen van de autorisatieprocedure. 3. Vastlegging van uitgevoerde controles op toegang tot de systemen.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q3 Actie 3: Q3				
11. Autorisaties: aanwijzen functionarissen		Geen overlap			
Beheersingsmaatregel	Er is een actuele lijst van, door de verwerkingsverantwoordelijke aangewezen, bevoegde functionarissen.				
Advies	Documenteer wat er moet gebeuren indien artikel 9 verwerkingen gaan plaatsvinden (bv het aanwijzen van bevoegd functionaris en de bijbehorende extra taken). Neem de beheersingsmaatregel op in 'Handboek Wet politiegegevens'.				
Actie	1. Opstellen van een regeling voor het geval artikel 9 Wpg verwerkingen gaan plaatsvinden en opname hiervan in het Handboek Wpg.				
Voortgang (verwijzing naar document)	Actie 1: Q2				
12. Onderscheid tussen verschillende categorieën van betrokkenen		Geen overlap			
Beheersingsmaatregel	De verwerkingsverantwoordelijke heeft geborgd dat, voor zover mogelijk, duidelijk onderscheid wordt gemaakt in de verschillende categorieën van betrokkenen.				
Advies	Beschrijf op welke wijze onderscheid wordt gemaakt tussen verdachten, slachtoffers en derden binnen de processen en applicaties, en zorg voor borging daarvan.				
Actie	1. Beschrijving van de wijze van onderscheid tussen betrokkenen binnen de processen en applicaties en opname hiervan in het register van verwerkingen. 2. Borging: jaarlijkse actualisering van het register van verwerkingen.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q3				
13. Verwerker en Verwerkersovereenkomst		BIO 15.1.1.3 P 20.5.1.3			
Beheersingsmaatregel	Bij uitbestedingen van taken moet de verwerker de verwerkingsverantwoordelijke alle informatie ter beschikking stellen om aantoonbaar te maken dat de afspraken in de verwerkersovereenkomst en de Wpg worden nageleefd. Er moeten specifieke afspraken gemaakt worden over de handelswijze bij een inbreuk op de beveiliging.				
Advies	Zorg voor een verwerkersovereenkomst met de leverancier van Carel, waarin Wpg eisen zijn meegenomen.				
Actie	1. Opstellen en vaststellen van een verwerkersovereenkomst met Eljakim die aan de Wpg voldoet.				
Voortgang (verwijzing naar document)	Actie 1: Q2				
14. Geheimhoudingsplicht		BIO 7.3.1.4			

Onderwerpen		BIO/Borgingsproduct Beheersingsmaatregel[3]	Externe audit 2022		
			Opzet	Bestaan	Werkin
		BIO 13.2.4.1			
Beheersingsmaatregel	Er is geborgd dat de boa of een andere persoon aan wie politiegegevens ter beschikking zijn gesteld formeel bekend is met de plicht tot geheimhouding en de consequenties bij schending van deze plicht.				
Advies	Zorg voor documentatie waaruit blijkt dat medewerkers de trainingen hebben gevolgd.				
Actie	1. Toon aan dat alle medewerkers een online training moeten doorlopen over privacy en informatiebeveiliging. 2. Zorg voor documentatie waaruit blijkt dat medewerkers de trainingen hebben gevolgd.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q2				
15. Geautomatiseerde individuele besluitvorming		P 20.4.2.3			
Beheersingsmaatregel	Besluiten die uitsluitend zijn gebaseerd op geautomatiseerde verwerking die voor de betrokkene nadelige rechtsgevolgen (kunnen) hebben 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 dat 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.				
Advies	Geen				
Actie	Geen				
Voortgang (verwijzing naar document)	n.v.t.				
16. Uitvoering van de dagelijkse politietaak		BIO 18.1.3.1			
Beheersingsmaatregel	Artikel 8-gegevens (zoals wildplassen, foutief aanbieden van afval, alcoholgebruik op de openbare weg: persoonsgegevens die worden verwerkt in het kader van de dagelijkse opsporingstaak) mogen tot 5 jaar na de eerste verwerkingsdatum met een gerichte zoekvraag worden geraadpleegd of verwerkt.				
Advies	Zorg voor de implementatie van het achter schot plaatsen van politiegegevens in Carel en Zaaksysteem na 1 jaar, waarna ze enkel nog beschikbaar zijn op hit-no-hit basis.				
Actie	1. Richt Citycontrol en Sharepoint aantoonbaar zo in dat politiegegeven alleen nog maar beschikbaar zijn op grond van een gerichte zoekvraag. 2. Voer een DPIA uit waar deze inrichting een onderdeel van is.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q2				
17. Ter beschikking stellen van politie-gegevens binnen het WPG-domein		P 20.4.6.6			
Beheersingsmaatregel	Verdere verwerking (dus met een ander doel dan het aanvankelijke verwerkingsdoel) van artikel 9-politiegegevens mag alleen na toestemming van de daartoe bevoegde functionaris plaatsvinden.				
Advies	Geen				
Actie	1. Stel een werkwijze op voor het geval van verdere verwerking van artikel 9 gegevens waarin de instemming van de bevoegd functionaris wordt vastgelegd.				
Voortgang (verwijzing naar document)	Actie 1: Q2				
18. Geautomatiseerd vergelijken en in combinatie zoeken		P 20.4.2.3			
Beheersingsmaatregel	Politiegegevens kunnen worden vergeleken met andere politiegegevens met als doel om vast te stellen of verbanden bestaan tussen de betreffende gegevens. De verwerkingsmogelijkheden geautomatiseerd vergelijken en in combinatie zoeken zijn gebonden aan strikte criteria (zie artikel 11 Wpg)				

Onderwerpen		BIO/Borgingsproduct Beheersingsmaatregel[3]	Externe audit 2022		
			Opzet	Bestaan	Werkin
Advies	Geen				
Actie	1. Stel een werkwijze op voor het geval vergelijking met andere politiegegevens met als doel om vast te stellen of verbanden bestaan tussen de betreffende gegevens.				
Voortgang (verwijzing naar document)	Actie 1: Q2				
19. Ondersteunende taken		Geen overlap			
Beheersingsmaatregel	De mogelijkheid bestaat om gegevens die oorspronkelijk zijn verwerkt op basis van artikel 8 of 9 verder te verwerken via een artikel 13-verwerking. Geborgd is dat voor de verwerkingen bedoeld in art 13 lid 1t/m 3, van tevoren is voldaan aan de schriftelijke vereisten (art 13 lid 4). Vooralsnog zijn er geen gevallen bekend van artikel 13-verwerkingen voor Boa's. Er wordt verwacht dat dit in de toekomst wel gaat gebeuren.				
Advies	Geen				
Actie	1. Stel een werkwijze op voor de borging dat voor de verwerkingen bedoeld in art 13 lid 1t/m 3, van tevoren is voldaan aan de schriftelijke vereisten (art 13 lid 4).				
Voortgang (verwijzing naar document)	Actie 1: Q2				
20. Bewaartermijnen, verwijderen en vernietigen		BIO 18.1.3.1			
Beheersingsmaatregel	Politiegegevens mogen niet langer worden bewaard dan is vastgelegd in wet- en regelgeving, of voor de doeleinden waarvoor deze zijn verwerkt. Het is aan de verwerkingsverantwoordelijke om ervoor te zorgen dat de gegevens conform de wet worden gecontroleerd, verwijderd en vernietigd.				
Advies	1. Stel in documentatie vast hoe is geborgd dat politiegegevens worden verwijderd en vernietigd conform de Wet politiegegevens. 2. Zorg voor gedocumenteerd bewijs van uitgevoerde verwijderacties.				
Actie	1. Stel een werkwijze op waarin is opgenomen dat politiegegevens worden verwijderd en vernietigd conform de Wpg . Maak daarbij inzichtelijk waar en hoe de gegevens zijn opgeslagen (systemen, archieven, back-ups, overige media), welke typen gegevens vanaf welk moment hoe lang worden bewaard en of en zo ja hoe controlemaatregelen zijn ingericht (geautomatiseerd of handmatig) die ervoor zorgen dat de verschillende typen gegevens op het juiste moment worden verwijderd. 2. Overleg bewijs van uitgevoerde verwijderacties.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q2				
21. Verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee					
Beheersingsmaatregel	Het delen van politiegegevens buiten het Wpg-domein mag alleen onder bepaalde voorwaarden plaatsvinden.				
Advies	Zorg voor documentatie waaruit blijkt dat de beheersmaatregelen in de praktijk zijn toegepast. Beschrijf een procedure voor het in kennis stellen van de ontvanger van politiegegevens indien geconstateerd wordt dat onjuiste politiegegevens zijn verstrekt of dat politiegegevens op onrechtmatig wijze zijn verstrekt. Zorg voor een overzicht van instanties waar verstrekkingen aan plaatsvinden zoals bedoeld in deze beheersmaatregel en artikelen.				
Actie	1. Stel vast of het overzicht van instanties waar verstrekkingen aan plaatsvinden volledig is. Ga daarbij onder meer in op bijv. de burgemeester, de Belastingdienst of het CJIB. 2. Stel een werkwijze/procedure op waaruit blijkt dat in geval van verstrekkingen aan de voorwaarden van deze Beheersingsmaatregel wordt voldaan. 3. Als blijkt dat er verstrekkingen plaatsvinden: toon aan dat aan de Beheersingsmaatregel wordt voldaan.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q2 Actie 3: Q3				

Onderwerpen		BIO/Borgingsproduct Beheersingsmaatregel[3]	Externe audit 2022		
			Opzet	Bestaan	Werkin
22. Doorgiften aan derde landen		P 20.2.6.2			
Beheersingsmaatregel	Het doorgeven van politiegegevens aan derde landen (alle landen buiten de EU, m.u.v. de landen in de EER – Noorwegen, Liechtenstein en IJsland) mag alleen onder bepaalde uitzonderingsgronden.				
Advies	Geen				
Actie	1. Formuleer hoe het eventueel doorgeven aan derde landen wordt getoetst aan de uitzonderingsgronden				
Voortgang (verwijzing naar document)	Actie 1: Q2				
23. Verstrekking aan derden structureel voor samenwerkingsverbanden		P 20.2.3.1			
Beheersingsmaatregel	Er zijn samenwerkingsverbanden waarbij politiegegevens worden verstrekt (bijvoorbeeld het RIEC). De verwerkingsverantwoordelijke moet vastleggen waarom deze verstrekking plaatsvindt.				
Advies	Stel vast of en documenteer welke samenwerkingsverbanden bestaan waarbij politiegegevens worden verstrekt zoals bedoeld in artikel 20 (betreffende organisaties die niet in het Besluit politiegegevens zijn opgenomen).				
Actie	1. Doe een steekproef om vast te stellen of voldoende is vastgelegd welke gegevensverstrekkingen hebben plaatsgevonden, wat daarvan het doel was, onder welke voorwaarden en aan wie de gegevens verstrekt zijn? 2. Stel vast welke samenwerkingsverbanden bestaan waarbij politiegegevens worden verstrekt zoals bedoeld in artikel 20 Wpg. 3. Stel vast of daarvoor convenanten zijn afgesloten en zo nee stel die vast.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q2 Actie 3: Q2				
24. Rechtstreekse verstrekking		BIO 13.2.1			
Beheersingsmaatregel	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				
Advies	Geen				
Actie	1. Beschrijf hoe eventuele rechtstreekse verstrekking plaatsvindt en hoe dat is geborgd.				
Voortgang (verwijzing naar document)	Actie 1: Q3				
25. Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering		P 20.4.1.3 P 20.4.3.2			
Beheersingsmaatregel	Verzoeken tot inzage, rectificatie, vernietiging van betrokkenen worden - met inachtneming van het gestelde in artikel 27 - tijdig en adequaat afgehandeld.				
Advies	Zorg voor vastlegging waaruit blijkt dat in de loop der jaren de privacyverklaring beschikbaar is op de website en dat uitvoering van de procedure rechten van betrokkenen aantoonbaar is uitgevoerd.				
Actie	Geen (domeinoverstijgend)				
Voortgang (verwijzing naar document)	n.v.t.				
26. Register		P 20.2.3.1			
Beheersingsmaatregel	De verwerkingsverantwoordelijke moet een Register van Verwerkingen bijhouden, waarin een aantal verplichte beschrijvingen moeten zijn opgenomen.				
Advies	Zorg voor consistentie in de bewaartermijnen voor vernietiging en verwijdering, in het document 'Handboek Wet politiegegevens'. Beschrijf bij de verwerkingen de naam en contactgegevens van de verwerkingsverantwoordelijke, de eventuele gezamenlijke				

Onderwerpen		BIO/Borgingsproduct Beheersingsmaatregel[3]	Externe audit 2022		
			Opzet	Bestaan	Werkin
	verwerkingsverantwoordelijke en de functionaris voor gegevensbescherming. Beschrijf voor alle verwerkingen de rechtsgrondslag en toekenning van autorisaties zoals bedoeld in artikel 6.				
Actie	1. Actualiseer het register van verwerkingen voor alle verplichte onderdelen in het domein				
Voortgang (verwijzing naar document)	Actie 1: Q3				
27. Documentatie		P 20.2.3.1			
Beheersingsmaatregel	De verwerkingsverantwoordelijke heeft een documentatieplicht. De documentatieplicht heeft niet alleen als doel het afleggen van verantwoording, maar ook het creëren van transparantie rondom de gegevensverwerkingen.				
Advies	Zorg voor invulling en uitvoering van de beheersmaatregelen welke betrekking hebben op artikel 32 lid l t/m 4 van de Wpg. Documenteer welke documentatie moet worden bijgehouden en hoe dat is ingericht binnen de organisatie.				
Actie	1. Inventariseer en documenteer welke documentatie moet worden bijgehouden en hoe dat is ingericht in de organisatie 2. Stel een procedure(s)/werkinstructie(s) voor de documentatieplicht op; 3. Toon aan met steekproeven dat aan de documentatieplicht en bijbehorende eisen wordt voldaan.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q2 Actie 3: Q2				
28. Logging		BIO 12.4.1 BIO 12.4.2 BIO 12.4.3			
Beheersingsmaatregel	De verwerkingsverantwoordelijke en de verwerker dragen zorg voor de logging van verwerkingen zoals opgenomen in art 32a lid l. 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.				
Advies	Zorg voor de inrichting en implementatie van een controleproces voor de periodieke beoordeling van logbestanden van systemen waarin politiegegevens worden verwerkt. Borg de bewaartermijnen van de logging ten behoeve van auditcontroles.				
Actie	1. Zorg ervoor dat het werkproces is ingericht en geïmplementeerd om de logbestanden periodiek te beoordelen; 2. Stel vast voor welke systemen de loggingsplicht van artikel 32a van toepassing is. 3. Toon aan dat conform het logging beleid wordt gewerkt. Ga daarbij in op: - de vraag of loggingbestanden beschikbaar zijn over de afgelopen verslagperiode, waarin de logregel minimaal het verzamelen, wijzigen, raadplegen, verstrekken (onder meer in de vorm van doorgiften), combineren is vastgelegd. - zijn de logbestanden voldoende beschermd tegen (ongeautoriseerde) wijzigingen?				
Voortgang (verwijzing naar document)	Actie 1: Q3 Actie 2: Q3 Actie 3: Q3				
29. Audits		BIO 18.2.1.2			
Beheersingsmaatregel	Er wordt uitvoering gegeven aan de eisen zoals gesteld in de Regeling Periodieke Audit politiegegevens.				
Advies	Zorg voor een vastgestelde auditplanning waaruit blijkt dat uitvoering wordt gegeven aan de eisen zoals gesteld in de Regeling Periodieke Audit politiegegevens (Rpap). Zorg voor de uitvoering van de relevante interne en externe audits conform de Rpap. Beschrijf bijvoorbeeld in het document 'Handboek Wet politiegegevens' ook de planning voor de volgens Rpap vereiste jaarlijkse interne audits.				
Actie	Geen (domeinoverstijgende actie)				

Onderwerpen		BIO/Borgingsproduct Beheersingsmaatregel[3]	Externe audit 2022		
			Opzet	Bestaan	Werkin
Voortgang (verwijzing naar document)	n.v.t.				
30. Melding datalekken		P 20.6.2.1 P 20.6.2.5			
Beheersingsmaatregel	De organisatie is verplicht om privacygerelateerde incidenten op gepaste wijze te detecteren en behandelen. Het beperken van de gevolgen en het nemen van maatregelen om toekomstige inbreuken te voorkomen staat hierbij centraal.				
Advies	Geen				
Actie	Geen				
Voortgang (verwijzing naar document)	n.v.t.				
31. Functionaris voor Gegevensbescherming		BIO 18.1.4.1 P 20.7.1.1			
Beheersingsmaatregel	Er moet een functionaris gegevensbescherming (FG) zijn aangesteld die toezicht houdt op het naleven van de Wpg, de uitvoering van DPIA's, de audits, de bewustmaking rondom de verwerking van politiegegevens, het toewijzen van de autorisaties en het beleid van de verwerkingsverantwoordelijke m.b.t. de bescherming van persoonsgegevens.				
Advies	Geen				
Actie	Geen (domeinoverstijgende actiepunten)				
Voortgang (verwijzing naar document)	n.v.t.				

Technische en organisatorische maatregelen		Conclusie		
		Opzet	Bestaan	Werking
1. Wijzigingenbeheer				
Beheersingsmaatregel	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.			
Advies	Zorg voor bewijsmateriaal over Onegov waaruit blijkt dat is voldaan aan de beheersmaatregel.			
Actie	1. Toon aan dat het wijzigingenbeheer wordt uitgevoerd voor de applicatie die wordt gebruikt.			
Voortgang (verwijzing naar document)	Actie 1: Q3			
2. Logische toegangsbeveiliging				
Beheersingsmaatregel	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.			
Advies	Zorg voor bewijsmateriaal waaruit blijkt dat is voldaan aan de beheersmaatregel.			
Actie	1. Stel een autorisatieprocedure op voor de applicatie die wordt gebruikt.			
Voortgang (verwijzing naar document)	Actie 1: Q2			
3. Beheer van kwetsbaarheden (patchmanagement)				
Beheersingsmaatregel	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.			

Technische en organisatorische maatregelen		Conclusie		
		Opzet	Bestaan	Werking
Advies	Zorg voor bewijsmateriaal waaruit blijkt dat is voldaan aan de beheersmaatregel.			
Actie	1. Stel een patchmanagement procedure op voor de applicatie die wordt gebruikt.			
Voortgang (verwijzing naar document)	Actie 1: Q3			
4. Cryptografie				
Beheersingsmaatregel	Ter bescherming van politiegegevens behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.			
Advies	Zorg voor bewijsmateriaal waaruit blijkt dat is voldaan aan de beheersmaatregel.			
Actie	1. Toon aan dat cryptografiebeleid van de gemeente wordt toegepast voor de applicatie die wordt gebruikt.			
Voortgang (verwijzing naar document)	Actie 1: Q3			
5. Vulnerability scans en Penetratietesten				
Beheersingsmaatregel	Penetratietesten en vulnerability scans worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de systemen waarin politiegegevens verwerkt worden.			
Advies	Zorg voor bewijs waaruit blijkt dat penetratietesten en vulnerabilityscans procesmatig en procedureel worden uitgevoerd.			
Actie	1. Vraag op bij de leverancier op welke wijze penetratietesten en vulnerabilityscans worden uitgevoerd.			
Voortgang (verwijzing naar document)	Actie 1: Q2			

Domein 5 Sociale Recherche

Legenda voor de beoordeling van de beheersmaatregelen	
Groen	Volledig opgezet, bestaan en/of effectief werken
Geel	Niet volledig opgezet, bestaan en/of effectief werken
Rood	Niet opgezet, bestaan en/of effectief werken
Grijs	Niet van toepassing

Onderwerpen		BIO/Borgingsproduct Beheersingsmaatregel[4]	Externe audit 2022		
			Opzet	Bestaan	Werkin
1. Reikwijdte		P 20.2.3.1 en P 20.2.3.4			
Beheersingsmaatregel	De verwerkingsverantwoordelijke heeft bestanden met politiegegevens binnen de organisatie geïdentificeerd en gedocumenteerd.				
Advies	Zorg voor vastlegging van de periodieke controle op de actualiteit van de vastlegging van bestanden met politiegegevens.				
Actie	1. Maak duidelijk welke gegevens en welke soorten verwerkingen van politiegegevens in Key2Handhaving en Sharepoint plaatsvinden en of deze verwerkingen enkel binnen die applicaties plaatsvinden. 2. De periodieke controle van verwerkingen van politiegegevens vindt jaarlijks in september/oktober plaats door de hoofden van het verantwoordelijke organisatieonderdeel op initiatief van de Privacy Officer. De Functionaris Gegevensbescherming houdt jaarlijks in oktober/november toezicht op de verwerking van politiegegevens in het kader van de Wpg. De controle en het toezicht vindt door middel van de jaarlijkse interne audit plaats. De privacy officer documenteert deze periodieke controle.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q3 en 4				
2. Doelbinding		P 20.2.3.1			
Beheersingsmaatregel	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.				
Advies	Het register en de doelen van de verwerkingen zijn gedocumenteerd in 'Handboek Wet politiegegevens' in 'BIJLAGE 1: HET REGISTER VAN VERWERKINGEN'. Zorg voor vastlegging van uitgevoerde controles dat bij het verwerken van politiegegevens altijd sprake is van doelbinding en dat de gegevens niet op een onrechtmatige wijze worden verwerkt. Bijvoorbeeld door het beschrijven wanneer en door wie een controle op verschillen in het verwerkingsregister en de huidige situatie heeft plaatsgevonden.				
Actie	1. De periodieke controle van verwerkingen van politiegegevens vindt jaarlijks in september/oktober plaats door de hoofden van het verantwoordelijke organisatieonderdeel op initiatief van de Privacy Officer. De Functionaris Gegevensbescherming houdt jaarlijks in oktober/november toezicht op de verwerking van politiegegevens in het kader van de Wpg. De controle en het toezicht vindt door middel van de jaarlijkse interne audit plaats. De privacy officer documenteert deze periodieke controle.				
Voortgang (verwijzing naar document)	Actie 1: Q3 en Q4				
3. Noodzakelijkheid en rechtmatigheid, vermelding herkomst					

[4] Voor de P-verwijzingen naar het Borgingsproduct, zie: https://www.informatiebeveiligingsdienst.nl/product/avg-borgingsproduct-2-0/ (Kolom F in tabblad Controls). Voor de BIO-verwijzingen, zie: https://www.informatiebeveiligingsdienst.nl/product/baseline-informatiebeveiliging-overheid-bio/

Onderwerpen		BIO/Borgingsproduct Beheersingsmaatregel[4]	Externe audit 2022		
			Opzet	Bestaan	Werkin
Beheersingsmaatregel	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.				
Advies	Zorg voor inhoudelijke controles op noodzakelijkheid en toereikendheid. Leg uitgevoerde controles vast, en op welke dossiers deze controles zijn uitgevoerd.				
Actie	1. Stel een procedure/werkinstructie op waaruit blijkt dat aan de Beheersingsmaatregel wordt voldaan. 2. De periodieke controle van verwerkingen van politiegegevens vindt jaarlijks in september/oktober plaats door de hoofden van het verantwoordelijke organisatieonderdeel op initiatief van de Privacy Officer. De Functionaris Gegevensbescherming houdt jaarlijks in oktober/november toezicht op de verwerking van politiegegevens in het kader van de Wpg. De controle en het toezicht vindt door middel van de jaarlijkse interne audit plaats. De privacy officer documenteert deze periodieke controle.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q3 en Q4				
4. Juistheid en volledigheid politiegegevens		P 20.7.1.3			
Beheersingsmaatregel	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.				
Advies	Richt controles in op kwaliteit ter borging van de juistheid en nauwkeurigheid van politiegegevens. Zorg voor documentatie waaruit blijkt dat dergelijke controles zijn uitgevoerd. Stel een procedure op voor de vernietiging van politiegegevens.				
Actie	1. Stel een procedure/werkinstructie op waaruit blijkt dat aan de Beheersingsmaatregel wordt voldaan en betrek hierbij de gemeentelijke archivaris. 2. Voer een DPIA uit.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q2				
5. Onderscheid feiten en oordeel		Geen overlap			
Beheersingsmaatregel	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.				
Advies	Zorg voor documentatie waaruit blijkt dat een periodieke controle op de uitvoering van de regel dat enkel feiten worden verwerkt heeft plaatsgevonden.				
Actie	1. Maak duidelijk dat bij het verwerken van politiegegevens voldoende inzichtelijk gemaakt is wat een vaststaand feit is, en wat een persoonlijk oordeel, bijvoorbeeld door labeling van de gegevens of een andere werkwijze. 2. De periodieke controle van verwerkingen van politiegegevens vindt jaarlijks in september/oktober plaats door de hoofden van het verantwoordelijke organisatieonderdeel op initiatief van de Privacy Officer. De Functionaris Gegevensbescherming houdt jaarlijks in oktober/november toezicht op de verwerking van politiegegevens in het kader van de Wpg. De controle en het toezicht vindt door middel van de jaarlijkse interne audit plaats. De privacy officer documenteert deze periodieke controle.				
Voortgang (verwijzing naar document)	Actie 1: Q 2 Actie 2: Q3 en 4				
6. Gegevensbescherming door beveiliging en ontwerp (privacy by design)		P 20.6.1.1 P 20.6.1.2 P 20.6.1.3			
Beheersingsmaatregel	Er is (aantoonbaar) een risicoanalyse uitgevoerd waaruit het risiconiveau blijkt met betrekking tot ongeoorloofde of onrechtmatige verwerking en tegen opzettelijk verlies, vernietiging of beschadiging.				

Onderwerpen		BIO/Borgingsproduct Beheersingsmaatregel[4]	Externe audit 2022		
			Opzet	Bestaan	Werkin
	De verwerkingsverantwoordelijke identificeert, evalueert en mitigeert systematisch en periodiek factoren die het beschermen van politiegegevens tegen ongeoorloofde of on rechtmatige 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 (bijvoorbeeld bij ontwikkelingen / wijzigingen).				
Advies	Voer een periodieke risicoanalyse uit en zorg voor een zichtbare relatie tussen de risico's en de genomen of te nemen maatregelen. Evalueer de maatregelen periodiek en leg de evaluatie vast. Zorg voor documentatie waaruit blijkt dat privacy by design is toegepast door de organisatie.				
Actie	1. Voer een DPIA uit. 2. Voer periodieke controle uit op autorisaties en logging v.w.b.t. verlies/vernietiging/beschadiging.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q2				
7. Gegevensbescherming door standaardinstellingen (privacy by default)		P 20.6.1.4 P 20.6.1.5			
Beheersingsmaatregel	De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen om te waarborgen dat standaard: ♦ 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.				
Advies	Zorg voor documentatie waaruit blijkt dat privacy by design/default is toegepast door de organisatie. Zorg voor documentatie waarin is vastgesteld onder welke voorwaarden toegang mag worden verschaft tot politiegegevens. Documenteer hoe is geborgd dat personen toegang hebben tot politiegegevens op basis van doelbinding (bv. periodieke controles).				
Actie	1. Voer een DPIA uit. 2. Voer periodieke controle uit op autorisaties en logging v.w.b.t. verlies/vernietiging/beschadiging. 3. Stel beleid op m.b.t. privacy by design en privacy by default.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q2 Actie 3: Q3				
8. Gegevensbeschermingseffectbeoordeling/ Data protection impact assessment (DPIA)		P 20.2.4.3			
Beheersingsmaatregel	Als een verwerking van persoonsgegevens waarschijnlijk een hoog risico oplevert voor de rechten en vrijheden van betrokkenen, moet een DPIA uitgevoerd worden. De DPIA brengt in kaart welke risico's er bestaan en bevat aanbevelingen voor het wegnemen van die risico's.				
Advies	Zorg voor vastlegging van de herbeoordeling van DPIA's. Voer DPIA's uit.				
Actie	1. Uitvoering van een DPIA. 2. Uitvoeren van de eventuele risicobeperkende maatregelen die daaruit voortvloeien.				
Voortgang (verwijzing naar document)	Actie 1:Q2 Actie 2: Q3				
9. Bijzondere categorieën van politiegegevens					
Beheersingsmaatregel	Er vindt geen verwerking van bijzondere categorieën van politiegegevens plaats, tenzij: ♦ Dat onvermijdelijk is voor het doel van de verwerking; ♦ Dit in aanvulling is op de verwerking van andere politiegegevens betreffende de persoon;				

Onderwerpen		BIO/Borgingsproduct Beheersingsmaatregel[4]	Externe audit 2022		
			Opzet	Bestaan	Werkin
	De gegevens afdoende zijn beveiligd.				
Advies	Beschrijf op welke wijze geborgd is dat geen bijzondere categorieën van politiegegevens worden verwerkt. Bijvoorbeeld met steekproeven op dossiers.				
Actie	1. Uitvoeren van een DPIA. 2. Uitvoeren van eventuele risicobeperkende maatregelen die daaruit voortvloeien.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q3				
10. Autorisaties en toegang tot politiegegevens		BIO 9.2.2.1 P 20.6.3.3			
Beheersingsmaatregel	Er is een systeem van autorisaties dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid.				
Advies	Zorg voor een autorisatieprocedure en -matrix waarin het Need to Know principe is opgenomen, en de wijze van uitvoering van de periodieke controle op toegang is opgenomen, en pas deze toe. Zorg voor vastlegging van uitgevoerde controles op toegang tot de systemen. Gebruik voor het opstellen van de autorisatieprocedure het document 'Bijlage 5 Beleid Logische Toegangsbeveiliging (vastgesteld door B en W d.d. 4-4-2018) (1)'.				
Actie	1. Autorisatiematrix opstellen en goedgekeurd door proceseigenaar. 2. Vaststellen van de autorisatieprocedure. 3. Vastlegging van uitgevoerde controles op toegang tot de systemen.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q3 Actie 3: Q3				
11. Autorisaties: aanwijzen functionarissen		Geen overlap			
Beheersingsmaatregel	Er is een actuele lijst van, door de verwerkingsverantwoordelijke aangewezen, bevoegde functionarissen.				
Advies	Documenteer wat er moet gebeuren indien artikel 9 verwerkingen gaan plaatsvinden (bv het aanwijzen van bevoegd functionaris en de bijbehorende extra taken). Neem de beheersingsmaatregel op in 'Handboek Wet politiegegevens'.				
Actie	1. Opstellen van een regeling voor het geval artikel 9 Wpg verwerkingen gaan plaatsvinden en opname hiervan in het Handboek Wpg.				
Voortgang (verwijzing naar document)	Actie 1: Q2				
12. Onderscheid tussen verschillende categorieën van betrokkenen		Geen overlap			
Beheersingsmaatregel	De verwerkingsverantwoordelijke heeft geborgd dat, voor zover mogelijk, duidelijk onderscheid wordt gemaakt in de verschillende categorieën van betrokkenen.				
Advies	Beschrijf op welke wijze onderscheid wordt gemaakt tussen verdachten, slachtoffers en derden binnen de processen en applicaties, en zorg voor borging daarvan.				
Actie	1. Beschrijving van de wijze van onderscheid tussen betrokkenen binnen de processen en applicaties en opname hiervan in het register van verwerkingen. 2. Borging: jaarlijkse actualisering van het register van verwerkingen.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q3				
13. Verwerker en Verwerkersovereenkomst		BIO 15.1.1.3 P 20.5.1.3			
Beheersingsmaatregel	Bij uitbestedingen van taken moet de verwerker de verwerkingsverantwoordelijke alle informatie ter beschikking stellen om aantoonbaar te maken dat de afspraken in de verwerkersovereenkomst en de Wpg worden nageleefd. Er moeten specifieke afspraken gemaakt worden over de handelswijze bij een inbreuk op de beveiliging.				
Advies	In het document 'Wpg interne audit domein 5' is beschreven dat een verwerkersovereenkomst niet nodig is voor Suite Key2Handhaving, gezien het een on remise applicatie betreft				
Actie	Geen				

Onderwerpen		BIO/Borgingsproduct Beheersingsmaatregel[4]	Externe audit 2022		
			Opzet	Bestaan	Werkin
Voortgang (verwijzing naar document)	n.v.t.				
14. Geheimhoudingsplicht		BIO 7.3.1.4 BIO 13.2.4.1			
Beheersingsmaatregel	Er is geborgd dat de boa of een andere persoon aan wie politiegegevens ter beschikking zijn gesteld formeel bekend is met de plicht tot geheimhouding en de consequenties bij schending van deze plicht.				
Advies	Zorg voor documentatie waaruit blijkt dat medewerkers de trainingen hebben gevolgd.				
Actie	1. Toon aan dat alle medewerkers een online training moeten doorlopen over privacy en informatiebeveiliging. 2. Zorg voor documentatie waaruit blijkt dat medewerkers de trainingen hebben gevolgd.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q2				
15. Geautomatiseerde individuele besluitvorming		P 20.4.2.3			
Beheersingsmaatregel	Besluiten die uitsluitend zijn gebaseerd op geautomatiseerde verwerking die voor de betrokkene nadelige rechtsgevolgen (kunnen) hebben 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 dat 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.				
Advies	Geen				
Actie	Geen				
Voortgang (verwijzing naar document)	n.v.t.				
16. Uitvoering van de dagelijkse politietaak		BIO 18.1.3.1			
Beheersingsmaatregel	Artikel 8-gegevens (zoals wildplassen, foutief aanbieden van afval, alcoholgebruik op de openbare weg: persoonsgegevens die worden verwerkt in het kader van de dagelijkse opsporingstaak) mogen tot 5 jaar na de eerste verwerkingsdatum met een gerichte zoekvraag worden geraadpleegd of verwerkt.				
Advies	In de interviews met de Senior Sociale Recherche en Boa Sociale Recherche van domein 5, de PO, CISO en FG is vastgesteld dat in Liaan alle politiegegevens beschikbaar bleven en niet achter schot werden geplaatst na 1 aar. In Key2Handhaving kan enkel worden gezocht op specifieke zaken. Beschrijf in documentatie hoe het hit-no-hits systeem is ingericht				
Actie	1. Voer een DPIA uit waar deze inrichting een onderdeel van is.				
Voortgang (verwijzing naar document)	Actie 1: Q2				
17. Ter beschikking stellen van politie-gegevens binnen het WPG-domein		P 20.4.6.6			
Beheersingsmaatregel	Verdere verwerking (dus met een ander doel dan het aanvankelijke verwerkingsdoel) van artikel 9-politiegegevens mag alleen na toestemming van de daartoe bevoegde functionaris plaatsvinden.				
Advies	Geen				
Actie	1. Stel een werkwijze op voor het geval van verdere verwerking van artikel 9 gegevens waarin de instemming van de bevoegd functionaris wordt vastgelegd.				
Voortgang (verwijzing naar document)	Actie 1: Q2				
18. Geautomatiseerd vergelijken en in combinatie zoeken		P 20.4.2.3			

Onderwerpen		BIO/Borgingsproduct Beheersingsmaatregel[4]	Externe audit 2022		
			Opzet	Bestaan	Werkin
Beheersingsmaatregel	Politiegegevens kunnen worden vergeleken met andere politiegegevens met als doel om vast te stellen of verbanden bestaan tussen de betreffende gegevens. De verwerkingsmogelijkheden geautomatiseerd vergelijken en in combinatie zoeken zijn gebonden aan strikte criteria (zie artikel 11 Wpg)				
Advies	Geen				
Actie	1. Stel een werkwijze op voor het geval vergelijking met andere politiegegevens met als doel om vast te stellen of verbanden bestaan tussen de betreffende gegevens.				
Voortgang (verwijzing naar document)	Actie 1: Q2				
19. Ondersteunende taken		Geen overlap			
Beheersingsmaatregel	De mogelijkheid bestaat om gegevens die oorspronkelijk zijn verwerkt op basis van artikel 8 of 9 verder te verwerken via een artikel 13-verwerking. Geborgd is dat voor de verwerkingen bedoeld in art 13 lid 1t/m 3, van tevoren is voldaan aan de schriftelijke vereisten (art 13 lid 4). Vooralsnog zijn er geen gevallen bekend van artikel 13-verwerkingen voor Boa's. Er wordt verwacht dat dit in de toekomst wel gaat gebeuren.				
Advies	Geen				
Actie	1. Stel een werkwijze op voor de borging dat voor de verwerkingen bedoeld in art 13 lid 1t/m 3, van tevoren is voldaan aan de schriftelijke vereisten (art 13 lid 4).				
Voortgang (verwijzing naar document)	Actie 1: Q2				
20. Bewaartermijnen, verwijderen en vernietigen		BIO 18.1.3.1			
Beheersingsmaatregel	Politiegegevens mogen niet langer worden bewaard dan is vastgelegd in wet- en regelgeving, of voor de doeleinden waarvoor deze zijn verwerkt. Het is aan de verwerkingsverantwoordelijke om ervoor te zorgen dat de gegevens conform de wet worden gecontroleerd, verwijderd en vernietigd.				
Advies	Stel in documentatie vast hoe is geborgd dat politiegegevens worden verwijderd en vernietigd conform de Wet politiegegevens. Zorg voor gedocumenteerd bewijs van uitgevoerde verwijderacties.				
Actie	1. Stel een werkwijze op waarin is opgenomen dat politiegegevens worden verwijderd en vernietigd conform de Wpg . Maak daarbij inzichtelijk waar en hoe de gegevens zijn opgeslagen (systemen, archieven, back-ups, overige media), welke typen gegevens vanaf welk moment hoe lang worden bewaard en of en zo ja hoe controlemaatregelen zijn ingericht (geautomatiseerd of handmatig) die ervoor zorgen dat de verschillende typen gegevens op het juiste moment worden verwijderd. 2. Overleg bewijs van uitgevoerde verwijderacties.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q2				
21. Verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee					
Beheersingsmaatregel	Het delen van politiegegevens buiten het Wpg-domein mag alleen onder bepaalde voorwaarden plaatsvinden.				
Advies	Zorg voor documentatie waaruit blijkt dat de beheersmaatregelen in de praktijk zijn toegepast. Beschrijf een procedure voor het in kennis stellen van de ontvanger van politiegegevens indien geconstateerd wordt dat onjuiste politiegegevens zijn verstrekt of dat politiegegevens op onrechtmatig wijze zijn verstrekt. Zorg voor een overzicht van instanties waar verstrekkingen aan plaatsvinden zoals bedoeld in deze beheersmaatregel en artikelen.				
Actie	1. Stel vast of het overzicht van instanties waar verstrekkingen aan plaatsvinden volledig is. Ga daarbij onder meer in op bijv. de burgemeester, de Belastingdienst of het CJIB. 2. Stel een werkwijze/procedure op waaruit blijkt dat in geval van verstrekkingen aan de voorwaarden van deze Beheersingsmaatregel wordt voldaan.				

Onderwerpen		BIO/Borgingsproduct Beheersingsmaatregel[4]	Externe audit 2022		
			Opzet	Bestaan	Werkin
	3. Als blijkt dat er verstrekkingen plaatsvinden: toon aan dat aan de Beheersingsmaatregel wordt voldaan.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q2 Actie 3: Q3				
22. Doorgiften aan derde landen		P 20.2.6.2			
Beheersingsmaatregel	Het doorgeven van politiegegevens aan derde landen (alle landen buiten de EU, m.u.v. de landen in de EER – Noorwegen, Liechtenstein en IJsland) mag alleen onder bepaalde uitzonderingsgronden.				
Advies	Geen				
Actie	1. Formuleer hoe het eventueel doorgeven aan derde landen wordt getoetst aan de uitzonderingsgronden.				
Voortgang (verwijzing naar document)	Actie 1: Q2				
23. Verstrekking aan derden structureel voor samenwerkingsverbanden		P 20.2.3.1			
Beheersingsmaatregel	Er zijn samenwerkingsverbanden waarbij politiegegevens worden verstrekt (bijvoorbeeld het RIEC). De verwerkingsverantwoordelijke moet vastleggen waarom deze verstrekking plaatsvindt.				
Advies	Stel vast of en documenteer welke samenwerkingsverbanden bestaan waarbij politiegegevens worden verstrekt zoals bedoeld in artikel 20 (betreffende organisaties die niet in het Besluit politiegegevens zijn opgenomen).				
Actie	1. Doe een steekproef om vast te stellen of voldoende is vastgelegd welke gegevensverstrekkingen hebben plaatsgevonden, wat daarvan het doel was, onder welke voorwaarden en aan wie de gegevens verstrekt zijn. 2. Stel vast welke samenwerkingsverbanden bestaan waarbij politiegegevens worden verstrekt zoals bedoeld in artikel 20 Wpg. 3. Stel vast of daarvoor convenanten zijn afgesloten en zo nee stel die vast.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q2 Actie 3: Q2				
24. Rechtstreekse verstrekking		BIO 13.2.1			
Beheersingsmaatregel	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				
Advies	Geen				
Actie	1. Beschrijf hoe eventuele rechtstreekse verstrekking plaatsvindt en hoe dat is geborgd.				
Voortgang (verwijzing naar document)	Actie 1: Q3				
25. Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering		P 20.4.1.3 P 20.4.3.2			
Beheersingsmaatregel	Verzoeken tot inzage, rectificatie, vernietiging van betrokkenen worden - met inachtneming van het gestelde in artikel 27 - tijdig en adequaat afgehandeld.				
Advies	Zorg voor vastlegging waaruit blijkt dat in de loop der jaren de privacyverklaring beschikbaar is op de website en dat uitvoering van de procedure rechten van betrokkenen aantoonbaar is uitgevoerd.				
Actie	Geen (domeinoverstijgend)				
Voortgang (verwijzing naar document)	n.v.t.				
26. Register		P 20.2.3.1			

Onderwerpen		BIO/Borgingsproduct Beheersingsmaatregel[4]	Externe audit 2022		
			Opzet	Bestaan	Werkin
Beheersingsmaatregel	De verwerkingsverantwoordelijke moet een Register van Verwerkingen bijhouden, waarin een aantal verplichte beschrijvingen moeten zijn opgenomen.				
Advies	Zorg voor consistentie in de bewaartermijnen voor vernietiging en verwijdering, in het document 'Handboek Wet politiegegevens'. Beschrijf bij de verwerkingen de naam en contactgegevens van de verwerkingsverantwoordelijke, de eventuele gezamenlijke verwerkingsverantwoordelijke en de functionaris voor gegevensbescherming. Beschrijf voor alle verwerkingen de rechtsgrondslag en toekenning van autorisaties zoals bedoeld in artikel 6.				
Actie	1. Actualiseer het register van verwerkingen voor alle verplichte onderdelen in het domein.				
Voortgang (verwijzing naar document)	Actie 1: Q3				
27. Documentatie		P 20.2.3.1			
Beheersingsmaatregel	De verwerkingsverantwoordelijke heeft een documentatieplicht. De documentatieplicht heeft niet alleen als doel het afleggen van verantwoording, maar ook het creëren van transparantie rondom de gegevensverwerkingen.				
Advies	Zorg voor invulling en uitvoering van de beheersmaatregelen welke betrekking hebben op artikel 32 lid l t/m 4 van de Wpg. Documenteer welke documentatie moet worden bijgehouden en hoe dat is ingericht binnen de organisatie.				
Actie	1. Inventariseer en documenteer welke documentatie moet worden bijgehouden en hoe dat is ingericht in de organisatie. 2. Stel een procedure(s)/werkinstructie(s) voor de documentatieplicht op. 3. Toon aan met steekproeven dat aan de documentatieplicht en bijbehorende eisen wordt voldaan.				
Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q2 Actie 3: Q2				
28. Logging		BIO 12.4.1 BIO 12.4.2 BIO 12.4.3			
Beheersingsmaatregel	De verwerkingsverantwoordelijke en de verwerker dragen zorg voor de logging van verwerkingen zoals opgenomen in art 32a lid l. 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.				
Advies	Zorg voor vastlegging over wat moet worden en wat wordt gelogd binnen de applicatie. Zorg voor de mogelijkheid van een steekproef van logregels waaruit lijkt dat deze logging over de periode 9 maart 2019 t/m 31 december 2021 beschikbaar was voor Liaan. Borg de bewaartermijnen van de logging ten behoeve van auditcontroles voor Key2Handhaving.				
Actie	1. Zorg ervoor dat het werkproces is ingericht en geïmplementeerd om de logbestanden periodiek te beoordelen; 2. Stel vast voor welke systemen de loggingsplicht van artikel 32a van toepassing is. 3. Toon aan dat conform het logging beleid wordt gewerkt. Ga daarbij in op: - de vraag of loggingbestanden beschikbaar zijn over de afgelopen verslagperiode, waarin in de logregel minimaal het verzamelen, wijzigen, raadplegen, verstrekken (onder meer in de vorm van doorgiften), combineren is vastgelegd. - zijn de logbestanden voldoende beschermd tegen (ongeautoriseerde) wijzigingen?				
Voortgang (verwijzing naar document)	Actie 1: Q3 Actie 2: Q3 Actie 3: Q3				
29. Audits		BIO 18.2.1.2			
Beheersingsmaatregel	Er wordt uitvoering gegeven aan de eisen zoals gesteld in de Regeling Periodieke Audit politiegegevens.				

Onderwerpen		BIO/Borgingsproduct Beheersingsmaatregel[4]	Externe audit 2022		
			Opzet	Bestaan	Werkin
Advies	Zorg voor een vastgestelde auditplanning waaruit blijkt dat uitvoering wordt gegeven aan de eisen zoals gesteld in de Regeling Periodieke Audit politiegegevens (Rpap). Zorg voor de uitvoering van de relevante interne en externe audits conform de Rpap. Beschrijf bijvoorbeeld in het document 'Handboek Wet politiegegevens' ook de planning voor de volgens Rpap vereiste jaarlijkse interne audits.				
Actie	Geen (domeinoverstijgende actie)				
Voortgang (verwijzing naar document)	n.v.t.				
30. Melding datalekken		P 20.6.2.1 P 20.6.2.5			
Beheersingsmaatregel	De organisatie is verplicht om privacygerelateerde incidenten op gepaste wijze te detecteren en behandelen. Het beperken van de gevolgen en het nemen van maatregelen om toekomstige inbreuken te voorkomen staat hierbij centraal.				
Advies	Geen				
Actie	Geen				
Voortgang (verwijzing naar document)	n.v.t.				
31. Functionaris voor Gegevensbescherming		BIO 18.1.4.1 P 20.7.1.1			
Beheersingsmaatregel	Er moet een functionaris gegevensbescherming (FG) zijn aangesteld die toezicht houdt op het naleven van de Wpg, de uitvoering van DPIA's, de audits, de bewustmaking rondom de verwerking van politiegegevens, het toewijzen van de autorisaties en het beleid van de verwerkingsverantwoordelijke m.b.t. de bescherming van persoonsgegevens.				
Advies	Geen				
Actie	Geen (domeinoverstijgende actiepunten)				
Voortgang (verwijzing naar document)	n.v.t.				

Technische en organisatorische maatregelen		Conclusie		
		Opzet	Bestaan	Werking
1. Wijzigingenbeheer				
Beheersingsmaatregel	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.			
Advies	Zorg voor bewijsvoering waaruit blijkt dat wijzigingenbeheer procesmatig en procedureel wordt uitgevoerd door de gemeente Venlo			
Actie	1. Stel een wijzigingenbeheer procedure op voor Key2Handhaving en toon aan dat conform die procedure wordt gewerkt.			
Voortgang (verwijzing naar document)	Actie 1: Q3			
2. Logische toegangsbeveiliging				
Beheersingsmaatregel	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.			
Advies	Zorg voor een gedocumenteerde autorisatieprocedure voor Key2Handhaving.			
Actie	1. Stel een autorisatieprocedure voor Key2Handhaving op.			
Voortgang (verwijzing naar document)	Actie 1: Q2			

Technische en organisatorische maatregelen		Conclusie		
		Opzet	Bestaan	Werking
3. Beheer van kwetsbaarheden (patchmanagement)				
Beheersingsmaatregel	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.			
Advies	Documenteer voor Key2Handhaving hoe tijdig informatie wordt verkregen over technische kwetsbaarheden en hoe daar op moet worden gereageerd (patchmanagement beleid/procedure).			
Actie	1. Stel een patchmanagement procedure op voor Key2Handhaving.			
Voortgang (verwijzing naar document)	Actie 1: Q3			
4. Cryptografie				
Beheersingsmaatregel	Ter bescherming van politiegegevens behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.			
Advies	Documenteer en implementeer een beleid voor het gebruik van cryptografische beheersmaatregelen.			
Actie	1. Toon aan dat cryptografiebeleid van de gemeente wordt toegepast voor de applicatie die wordt gebruikt.			
Voortgang (verwijzing naar document)	Actie 1: Q3			
5. Vulnerability scans en Penetratietesten				
Beheersingsmaatregel	Penetratietesten en vulnerability scans worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de systemen waarin politiegegevens verwerkt worden.			
Advies	Zorg voor bewijs waaruit blijkt dat penetratietesten en vulnerabilityscans procesmatig en procedureel worden uitgevoerd voor de gemeente Venlo (Voor de gemeente Venlo is niet vastgesteld of penetratietesten en vulnerability scans procesmatig en procedureel worden uitgevoerd. De gemeente Venlo is deels zelf beheerder van de applicatie.)			
Actie	1. Toon aan op welke wijze penetratietesten en vulnerabilityscans worden uitgevoerd door de gemeente Venlo voor Key2Handhaving.			
Voortgang (verwijzing naar document)	Actie 1: Q2			

Domeinoverstijgende acties

Legenda voor de beoordeling van de beheersmaatregelen	
Groen	Volledig opgezet, bestaan en/of effectief werken
Geel	Niet volledig opgezet, bestaan en/of effectief werken
Rood	Niet opgezet, bestaan en/of effectief werken
Grijs	Niet van toepassing

Onderwerpen	BIO/Borgingsproduct Beheersingsmaatregel[5]	Externe audit 2022

[5] Voor de P-verwijzingen naar het Borgingsproduct, zie: https://www.informatiebeveiligingsdienst.nl/product/avg-borgingsproduct-2-0/ (Kolom F in tabblad Controls). Voor de BIO-verwijzingen, zie: https://www.informatiebeveiligingsdienst.nl/product/baseline-informatiebeveiliging-overheid-bio/

			Opzet	Bestaan	Werkin
1. Reikwijdte		P 20.2.3.1 en P 20.2.3.4			
Beheersingsmaatregel	De verwerkingsverantwoordelijke heeft bestanden met politiegegevens binnen de organisatie geïdentificeerd en gedocumenteerd.				
Advies	Zorg voor vastlegging van de periodieke controle op de actualiteit van de vastlegging van bestanden met politiegegevens.				
Actie	1. De periodieke controle van verwerkingen van politiegegevens vindt jaarlijks in september/oktober plaats door de hoofden van het verantwoordelijke organisatieonderdeel op initiatief van de Privacy Officer. De Functionaris Gegevensbescherming houdt jaarlijks in oktober/november toezicht op de verwerking van politiegegevens in het kader van de Wpg. De controle en het toezicht vindt door middel van de jaarlijkse interne audit plaats. De privacy officer documenteert deze periodieke controle. 2. Neem deze periodieke controle op in een auditplan.				
Voortgang (verwijzing naar document)	Actie 1: Q3 en 4 (FG en PO) Actie 2: Q2 (FG)				
2. Doelbinding		P 20.2.3.1			
Beheersingsmaatregel	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.				
Advies	Het register en de doelen van de verwerkingen zijn gedocumenteerd in 'Handboek Wet politiegegevens' in 'BIJLAGE 1: HET REGISTER VAN VERWERKINGEN'. Zorg voor vastlegging van uitgevoerde controles dat bij het verwerken van politiegegevens altijd sprake is van doelbinding en dat de gegevens niet op een onrechtmatige wijze worden verwerkt. Bijvoorbeeld door het beschrijven wanneer en door wie een controle op verschillen in het verwerkingsregister en de huidige situatie heeft plaatsgevonden.				
Actie	Cf actie Reikwijdte (zie onder 1)				
Voortgang (verwijzing naar document)	Cf actie Reikwijdte (zie onder 1)				
3. Noodzakelijkheid en rechtmatigheid, vermelding herkomst					
Beheersingsmaatregel	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.				
Advies	Zorg voor inhoudelijke controles op noodzakelijkheid en toereikendheid. Leg uitgevoerde controles vast, en op welke dossiers deze controles zijn uitgevoerd.				
Actie	Cf. actie reikwijdte (zie onder 1)				
Voortgang (verwijzing naar document)	Cf. actie Reikwijdte (zie onder 1)				
4. Juistheid en volledigheid politiegegevens		P 20.7.1.3			
Beheersingsmaatregel	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.				
Advies	Richt controles in op kwaliteit ter borging van de juistheid en nauwkeurigheid van politiegegevens. Zorg voor documentatie waaruit blijkt dat dergelijke controles zijn uitgevoerd. Stel een procedure op voor de vernietiging van politiegegevens.				
Actie	1. Voer een DPIA uit (ondersteund door de PO en met advies van CISO en FG). 2. Houdt controle op de uitvoering van de maatregelen die hieruit voortvloeien.				
Voortgang (verwijzing naar document)	Actie 1: n.v.t. (domein specifiek) Actie 2: Q3 (FG)				
5. Onderscheid feiten en oordeel		Geen overlap			
Beheersingsmaatregel	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.
Advies	Zorg voor documentatie waaruit blijkt dat een periodieke controle op de uitvoering van de regel dat enkel feiten worden verwerkt heeft plaatsgevonden.
Actie	Cf actie Reikwijdte
Voortgang (verwijzing naar document)	Cf actie Reikwijdte
6. Gegevensbescherming door beveiliging en ontwerp (privacy by design)	P 20.6.1.1 P 20.6.1.2 P 20.6.1.3
Beheersingsmaatregel	Er is (aantoonbaar) een risicoanalyse uitgevoerd waaruit het risiconiveau blijkt met betrekking tot ongeoorloofde of onrechtmatige verwerking en tegen opzettelijk verlies, vernietiging of beschadiging. De verwerkingsverantwoordelijke identificeert, evalueert en mitigeert systematisch en periodiek factoren die het beschermen van politiegegevens tegen ongeoorloofde of on rechtmatige 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 (bijvoorbeeld bij ontwikkelingen / wijzigingen).
Advies	Voer een periodieke risicoanalyse uit en zorg voor een zichtbare relatie tussen de risico's en de genomen of te nemen maatregelen. Evalueer de maatregelen periodiek en leg de evaluatie vast. Zorg voor documentatie waaruit blijkt dat privacy by design is toegepast door de organisatie.
Actie	1. Voer een DPIA uit (ondersteund door de PO en met advies van CISO en FG). 2. Houdt controle op de uitvoering van de maatregelen die hieruit voortvloeien. 3. Stel beleid op met betrekking tot privacy by design.
Voortgang (verwijzing naar document)	Actie 1: n.v.t. (domeinspecifiek) Actie 2: Q3 (FG) Actie 3: PO en CISO
7. Gegevensbescherming door standaardinstellingen (privacy by default)	P 20.6.1.4 P 20.6.1.5
Beheersingsmaatregel	De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen om te waarborgen dat standaard: ♦ 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.
Advies	Zorg voor documentatie waaruit blijkt dat privacy by design/default is toegepast door de organisatie. Zorg voor documentatie waarin is vastgesteld onder welke voorwaarden toegang mag worden verschaft tot politiegegevens. Documenteer hoe is geborgd dat personen toegang hebben tot politiegegevens op basis van doelbinding (bv. periodieke controles).
Actie	1. Voer een DPIA uit (ondersteund door de PO en met advies van CISO en FG). 2. Houdt controle op de uitvoering van de maatregelen die hieruit voortvloeien. 3. Stel beleid op met betrekking tot privacy by default.
Voortgang (verwijzing naar document)	Actie 1: n.v.t. (domeinspecifiek) Actie 2: Q3 (FG) Actie 3: Q3
8. Gegevensbeschermingseffectbeoordeling/ Data protection impact assessment (DPIA)	P 20.2.4.3
Beheersingsmaatregel	Als een verwerking van persoonsgegevens waarschijnlijk een hoog risico oplevert voor de rechten en vrijheden van betrokkenen, moet een DPIA uitgevoerd worden. De DPIA brengt in kaart welke risico's er bestaan en bevat aanbevelingen voor het wegnemen van die risico's.
Advies	Zorg voor vastlegging van de herbeoordeling van DPIA's. Voer DPIA's uit.

Actie	1. Voer een DPIA uit (ondersteund door de PO en met advies van CISO en FG). 2. Houdt controle op de uitvoering van de maatregelen die hieruit voortvloeien.
Voortgang (verwijzing naar document)	Actie 1: n.v.t. (domeinspecifiek) Actie 2: Q3 (FG)
9. Bijzondere categorieën van politiegegevens	
Beheersingsmaatregel	Er vindt geen verwerking van bijzondere categorieën van politiegegevens plaats, tenzij: ♦ 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.
Advies	Beschrijf op welke wijze geborgd is dat geen bijzondere categorieën van politiegegevens worden verwerkt. Bijvoorbeeld met steekproeven op dossiers.
Actie	1. Voer een DPIA uit (ondersteund door de PO en met advies van CISO en FG). 2. Houdt controle op de uitvoering van de maatregelen die hieruit voortvloeien.
Voortgang (verwijzing naar document)	Actie 1: n.v.t. (domeinspecifiek) Actie 2: Q3 (FG)
10. Autorisaties en toegang tot politiegegevens	BIO 9.2.2.1 P 20.6.3.3
Beheersingsmaatregel	Er is een systeem van autorisaties dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid.
Advies	Zorg voor een autorisatieprocedure en -matrix waarin het Need to Know principe is opgenomen, en de wijze van uitvoering van de periodieke controle op toegang is opgenomen, en pas deze toe. Zorg voor vastlegging van uitgevoerde controles op toegang tot de systemen. Gebruik voor het opstellen van de autorisatieprocedure het document 'Bijlage 5 Beleid Logische Toegangsbeveiliging (vastgesteld door B en W d.d. 4-4-2018) (1)'.
Actie	1. Vaststellen van de autorisatieprocedure. 2. Vastlegging van uitgevoerde controles op toegang tot de systemen.
Voortgang (verwijzing naar document)	Actie 1: Q2 (CISO) Actie 2: Q3 (CISO)
11. Autorisaties: aanwijzen functionarissen	Geen overlap
Beheersingsmaatregel	Er is een actuele lijst van, door de verwerkingsverantwoordelijke aangewezen, bevoegde functionarissen.
Advies	Documenteer wat er moet gebeuren indien artikel 9 verwerkingen gaan plaatsvinden (bv het aanwijzen van bevoegd functionaris en de bijbehorende extra taken). Neem de beheersingsmaatregel op in 'Handboek Wet politiegegevens'.
Actie	1. Opstellen van een regeling voor het geval artikel 9 Wpg verwerkingen gaan plaatsvinden. 2. Opname hiervan in het Handboek Wpg.
Voortgang (verwijzing naar document)	Actie 1: Q2 (PO) Actie 2: Q3 (PO)
12. Onderscheid tussen verschillende categorieën van betrokkenen	Geen overlap
Beheersingsmaatregel	De verwerkingsverantwoordelijke heeft geborgd dat, voor zover mogelijk, duidelijk onderscheid wordt gemaakt in de verschillende categorieën van betrokkenen.
Advies	Beschrijf op welke wijze onderscheid wordt gemaakt tussen verdachten, slachtoffers en derden binnen de processen en applicaties, en zorg voor borging daarvan.
Actie	1. Beschrijving van de wijze van onderscheid tussen betrokkenen binnen de processen en applicaties en de borging hiervan. 2. Betrek deze beschrijving bij de uit te voeren DPIA's.
Voortgang (verwijzing naar document)	n.v.t. (domeinspecifiek)
13. Verwerker en Verwerkersovereenkomst	BIO 15.1.1.3 P 20.5.1.3
Beheersingsmaatregel	Bij uitbestedingen van taken moet de verwerker de verwerkingsverantwoordelijke alle informatie ter beschikking stellen om aantoonbaar te maken dat de afspraken in de verwerkersovereenkomst en de Wpg worden nageleefd. Er moeten specifieke afspraken gemaakt worden over de handelswijze bij een inbreuk op de beveiliging.

Advies	Zorg voor een verwerkersovereenkomst waarin Wpg eisen zijn meegenomen.		
Actie	Geen domeinoverstijgende maatregelen		
Voortgang (verwijzing naar document)	n.v.t.		
14. Geheimhoudingsplicht		BIO 7.3.1.4 BIO 13.2.4.1	
Beheersingsmaatregel	Er is geborgd dat de boa of een andere persoon aan wie politiegegevens ter beschikking zijn gesteld formeel bekend is met de plicht tot geheimhouding en de consequenties bij schending van deze plicht.		
Advies	Zorg voor documentatie waaruit blijkt dat medewerkers de trainingen hebben gevolgd.		
Actie	1. Jaarlijkse cursus voor Boa's organiseren (verplicht bij te wonen).		
Voortgang (verwijzing naar document)	Actie 1: Q3 (PO)		
15. Geautomatiseerde individuele besluitvorming		P 20.4.2.3	
Beheersingsmaatregel	Besluiten die uitsluitend zijn gebaseerd op geautomatiseerde verwerking die voor de betrokkene nadelige rechtsgevolgen (kunnen) hebben 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 dat 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.		
Advies	Geen		
Actie	Geen		
Voortgang (verwijzing naar document)	n.v.t.		
16. Uitvoering van de dagelijkse politietaak		BIO 18.1.3.1	
Beheersingsmaatregel	Artikel 8-gegevens (zoals wildplassen, foutief aanbieden van afval, alcoholgebruik op de openbare weg: persoonsgegevens die worden verwerkt in het kader van de dagelijkse opsporingstaak) mogen tot 5 jaar na de eerste verwerkingsdatum met een gerichte zoekvraag worden geraadpleegd of verwerkt.		
Advies	Zorg voor de implementatie van het achter schot plaatsen van politiegegevens na 1 jaar, waarna ze enkel nog beschikbaar zijn op hit-no-hit basis.		
Actie	1. Voer een DPIA uit waar deze inrichting een onderdeel van is.		
Voortgang (verwijzing naar document)	Actie 1: Q2		
17. Ter beschikking stellen van politie-gegevens binnen het WPG-domein		P 20.4.6.6	
Beheersingsmaatregel	Verdere verwerking (dus met een ander doel dan het aanvankelijke verwerkingsdoel) van artikel 9-politiegegevens mag alleen na toestemming van de daartoe bevoegde functionaris plaatsvinden.		
Advies	Geen		
Actie	1. Stel een werkwijze op voor het geval van verdere verwerking van artikel 9 gegevens waarin de instemming van de bevoegd functionaris wordt vastgelegd. 2. Neem deze werkwijze op in het Handboek Wpg.		
Voortgang (verwijzing naar document)	Actie 1: Q2 (PO) Actie 2: Q3 (PO)		
18. Geautomatiseerd vergelijken en in combinatie zoeken		P 20.4.2.3	
Beheersingsmaatregel	Politiegegevens kunnen worden vergeleken met andere politiegegevens met als doel om vast te stellen of verbanden bestaan tussen de betreffende gegevens. De verwerkingsmogelijkheden geautomatiseerd vergelijken en in combinatie zoeken zijn gebonden aan strikte criteria (zie artikel 11 Wpg)		
Advies	Geen		
Actie	1. Stel een werkwijze op voor het geval vergelijking met andere politiegegevens met als doel om vast te stellen of verbanden bestaan tussen de betreffende gegevens. 2. Neem deze werkwijze op in het Handboek Wpg.		

Voortgang (verwijzing naar document)	Actie 1: Q2 Actie 2: Q3
19. Ondersteunende taken	Geen overlap
Beheersingsmaatregel	De mogelijkheid bestaat om gegevens die oorspronkelijk zijn verwerkt op basis van artikel 8 of 9 verder te verwerken via een artikel 13-verwerking. Geborgd is dat voor de verwerkingen bedoeld in art 13 lid 1t/m 3, van tevoren is voldaan aan de schriftelijke vereisten (art 13 lid 4). Vooralsnog zijn er geen gevallen bekend van artikel 13-verwerkingen voor Boa's. Er wordt verwacht dat dit in de toekomst wel gaat gebeuren.
Advies	Geen
Actie	1. Stel een werkwijze op voor de borging dat voor de verwerkingen bedoeld in art 13 lid 1t/m 3, van tevoren is voldaan aan de schriftelijke vereisten (art 13 lid 4). 2. Neem deze werkwijze op in het Handboek Wpg.
Voortgang (verwijzing naar document)	Actie 1: Q3 (PO) Actie 2: Q3 (PO)
20. Bewaartermijnen, verwijderen en vernietigen	BIO 18.1.3.1
Beheersingsmaatregel	Politiegegevens mogen niet langer worden bewaard dan is vastgelegd in wet- en regelgeving, of voor de doeleinden waarvoor deze zijn verwerkt. Het is aan de verwerkingsverantwoordelijke om ervoor te zorgen dat de gegevens conform de wet worden gecontroleerd, verwijderd en vernietigd.
Advies	Stel in documentatie vast hoe is geborgd dat politiegegevens worden verwijderd en vernietigd conform de Wet politiegegevens. Zorg voor gedocumenteerd bewijs van uitgevoerde verwijderacties.
Actie	1. Stel een werkwijze op waarin is opgenomen dat politiegegevens worden verwijderd en vernietigd conform de Wpg . Maak daarbij inzichtelijk waar en hoe de gegevens zijn opgeslagen (systemen, archieven, back-ups, overige media), welke typen gegevens vanaf welk moment hoe lang worden bewaard en of en zo ja hoe controlemaatregelen zijn ingericht (geautomatiseerd of handmatig) die ervoor zorgen dat de verschillende typen gegevens op het juiste moment worden verwijderd. 2. Overleg bewijs van uitgevoerde verwijderacties.
Voortgang (verwijzing naar document)	n.v.t. (domeinspecifiek)
21. Verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee	
Beheersingsmaatregel	Het delen van politiegegevens buiten het Wpg-domein mag alleen onder bepaalde voorwaarden plaatsvinden.
Advies	Zorg voor documentatie waaruit blijkt dat de beheersmaatregelen in de praktijk zijn toegepast. Beschrijf een procedure voor het in kennis stellen van de ontvanger van politiegegevens indien geconstateerd wordt dat onjuiste politiegegevens zijn verstrekt of dat politiegegevens op onrechtmatig wijze zijn verstrekt. Zorg voor een overzicht van instanties waar verstrekkingen aan plaatsvinden zoals bedoeld in deze beheersmaatregel en artikelen.
Actie	1. Stel vast of het overzicht van instanties waar verstrekkingen aan plaatsvinden volledig is. 2. Stel een werkwijze/procedure op waaruit blijkt dat in geval van verstrekkingen aan de voorwaarden van deze Beheersingsmaatregel wordt voldaan. 3. Als blijkt dat er verstrekkingen plaatsvinden: toon aan dat aan de Beheersingsmaatregel wordt voldaan.
Voortgang (verwijzing naar document)	n.v.t. (domeinspecifiek)
22. Doorgiften aan derde landen	P 20.2.6.2
Beheersingsmaatregel	Het doorgeven van politiegegevens aan derde landen (alle landen buiten de EU, m.u.v. de landen in de EER – Noorwegen, Liechtenstein en IJsland) mag alleen onder bepaalde uitzonderingsgronden.
Advies	Geen
Actie	Geen
Voortgang (verwijzing naar document)	n.v.t.

23. Verstrekking aan derden structureel voor samenwerkingsverbanden	P 20.2.3.1
Beheersingsmaatregel	Er zijn samenwerkingsverbanden waarbij politiegegevens worden verstrekt (bijvoorbeeld het RIEC). De verwerkingsverantwoordelijke moet vastleggen waarom deze verstrekking plaatsvindt.
Advies	Stel vast of en documenteer welke samenwerkingsverbanden bestaan waarbij politiegegevens worden verstrekt zoals bedoeld in artikel 20 (betreffende organisaties die niet in het Besluit politiegegevens zijn opgenomen).
Actie	1. Doe een steekproef om vast te stellen of voldoende is vastgelegd welke gegevensverstrekkingen hebben plaatsgevonden, wat daarvan het doel was, onder welke voorwaarden en aan wie de gegevens verstrekt zijn? 2. Stel vast welke samenwerkingsverbanden bestaan waarbij politiegegevens worden verstrekt zoals bedoeld in artikel 20 Wpg. 3. Stel vast of daarvoor convenanten zijn afgesloten en zo nee stel die vast. 4. Neem deze op in het Handboek Wpg.
Voortgang (verwijzing naar document)	Actie 1: Q2 (PO, onderdeel van de DPIA) Actie 2: Q2 (PO, onderdeel van de DPIA) Actie 3: Q2 (PO, onderdeel van de DPIA), domeinspecifiek igv vaststellen evt. convenanten Actie 4: Q3 (PO)

24. Rechtstreekse verstrekking	BIO 13.2.1
Beheersingsmaatregel	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
Advies	Geen
Actie	Geen
Voortgang (verwijzing naar document)	n.v.t.

25. Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering	P 20.4.1.3 P 20.4.3.2
Beheersingsmaatregel	Verzoeken tot inzage, rectificatie, vernietiging van betrokkenen worden - met inachtneming van het gestelde in artikel 27 - tijdig en adequaat afgehandeld.
Advies	Zorg voor vastlegging waaruit blijkt dat in de loop der jaren de privacyverklaring beschikbaar is op de website en dat uitvoering van de procedure rechten van betrokkenen aantoonbaar is uitgevoerd.
Actie	1. Jaarlijks een printscreen van de website opnemen in het op te stellen. verantwoordingsdocument voor de interne audit. 2. Jaarlijkse rapportage over de uitvoering van de procedure rechten van betrokkenen in het op te stellen verantwoordingsdocument voor de interne audit.
Voortgang (verwijzing naar document)	Actie 1: Q3 (PO) Actie 2: Q2 (FG) in jaarverslag FG

26. Register	P 20.2.3.1
Beheersingsmaatregel	De verwerkingsverantwoordelijke moet een Register van Verwerkingen bijhouden, waarin een aantal verplichte beschrijvingen moeten zijn opgenomen.
Advies	Zorg voor consistentie in de bewaartermijnen voor vernietiging en verwijdering, in het document 'Handboek Wet politiegegevens'. Beschrijf bij de verwerkingen de naam en contactgegevens van de verwerkingsverantwoordelijke, de eventuele gezamenlijke verwerkingsverantwoordelijke en de functionaris voor gegevensbescherming. Beschrijf voor alle verwerkingen de rechtsgrondslag en toekenning van autorisaties zoals bedoeld in artikel 6.
Actie	1. Actualiseer het register van verwerkingen voor alle verplichte onderdelen in domein 1.
Voortgang (verwijzing naar document)	n.v.t. (domeinspecifiek)

27. Documentatie	P 20.2.3.1

Beheersingsmaatregel	De verwerkingsverantwoordelijke heeft een documentatieplicht. De documentatieplicht heeft niet alleen als doel het afleggen van verantwoording, maar ook het creëren van transparantie rondom de gegevensverwerkingen.
Advies	Zorg voor invulling en uitvoering van de beheersmaatregelen welke betrekking hebben op artikel 32 lid l t/m 4 van de Wpg. Documenteer welke documentatie moet worden bijgehouden en hoe dat is ingericht binnen de organisatie.
Actie	1. Inventariseer en documenteer welke documentatie moet worden bijgehouden en hoe dat is ingericht in de organisatie. 2. Stel een procedure(s)/werkinstructie(s) voor de documentatieplicht op. 3. Toon aan met steekproeven dat aan de documentatieplicht en bijbehorende eisen wordt voldaan.
Voortgang (verwijzing naar document)	Actie 1: Q2 (PO) Actie 2: Q2 (PO) Actie 3: Q2 (PO in de DPIA)

28. Logging	BIO 12.4.1 BIO 12.4.2 BIO 12.4.3			
Beheersingsmaatregel	De verwerkingsverantwoordelijke en de verwerker dragen zorg voor de logging van verwerkingen zoals opgenomen in art 32a lid l. 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.			
Advies	Zorg voor de inrichting en implementatie van een controleproces voor de periodieke beoordeling van logbestanden van systemen waarin politiegegevens worden verwerkt. Borg de bewaartermijnen van de logging ten behoeve van auditcontroles.			
Actie	1. Stel logging beleid op onder verantwoordelijkheid van de CISO waarbij ook een intern werkproces is ingericht en geïmplementeerd om de logbestanden periodiek te beoordelen. 2. Stel vast voor welke systemen de loggingsplicht van artikel 32a van toepassing is. 3. Toon aan dat conform het logging beleid wordt gewerkt. Ga daarbij in op: - de vraag of loggingbestanden beschikbaar zijn over de afgelopen verslagperiode, waarin de logregel minimaal het verzamelen, wijzigen, raadplegen, verstrekken (onder meer in de vorm van doorgiften), combineren is vastgelegd. - zijn de logbestanden voldoende beschermd tegen (ongeautoriseerde) wijzigingen?			
Voortgang (verwijzing naar document)	Actie 1: Q3 (CISO) Actie 2: Q3 (CISO) Actie 3: Q3 (CISO)			

29. Audits	BIO 18.2.1.2			
Beheersingsmaatregel	Er wordt uitvoering gegeven aan de eisen zoals gesteld in de Regeling Periodieke Audit politiegegevens.			
Advies	Zorg voor een vastgestelde auditplanning waaruit blijkt dat uitvoering wordt gegeven aan de eisen zoals gesteld in de Regeling Periodieke Audit politiegegevens (Rpap). Zorg voor de uitvoering van de relevante interne en externe audits conform de Rpap. Beschrijf bijvoorbeeld in het document 'Handboek Wet politiegegevens' ook de planning voor de volgens Rpap vereiste jaarlijkse interne audits.			
Actie	1. Stel een auditplanning vast voor de interne en externe Wpg audit. 2. Neem deze op in het handboek Wpg.			
Voortgang (verwijzing naar document)	Actie 1: Q2 (FG iom VIC) Actie 2: Q3 (PO)			

30. Melding datalekken	P 20.6.2.1 P 20.6.2.5			
Beheersingsmaatregel	De organisatie is verplicht om privacy gerelateerde incidenten op gepaste wijze te detecteren en behandelen. Het beperken van de gevolgen en het nemen van maatregelen om toekomstige inbreuken te voorkomen staat hierbij centraal.			
Advies	Geen			
Actie	Geen			
Voortgang (verwijzing naar document)	n.v.t.			

31. Functionaris voor Gegevensbescherming	BIO 18.1.4.1 P 20.7.1.1			
Beheersingsmaatregel	Er moet een functionaris gegevensbescherming (FG) zijn aangesteld die toezicht houdt op het naleven van de Wpg, de uitvoering van DPIA's, de audits, de bewustmaking rondom de verwerking van politiegegevens, het toewijzen van de autorisaties en het beleid van de verwerkingsverantwoordelijke m.b.t. de bescherming van persoonsgegevens.			
Advies	Geen			
Actie	1. Pas het statuut voor de FG aan met de Wpg. 2. Een jaarverslag van de FG wordt gedocumenteerd in 'Jaarverslag bescherming persoonsgegevens 2022'. Daarin wordt ook ingegaan op de Wpg. 3. Stel een auditplanning op. 4. De periodieke controle van verwerkingen van politiegegevens vindt jaarlijks in september/oktober plaats door de hoofden van het verantwoordelijke organisatieonderdeel op initiatief van de Privacy Officer. De Functionaris Gegevensbescherming houdt jaarlijks in oktober/november toezicht op de verwerking van politiegegevens in het kader van de Wpg. De controle en het toezicht vindt door middel van de jaarlijkse interne audit plaats. De privacy officer documenteert deze periodieke controle.			
Voortgang (verwijzing naar document)	Actie 1: Q2 (FG) Actie 2: Q2 (FG) Actie 3: Q2 (FG) Actie 2: Q4 (FG en PO)			

Technische en organisatorische maatregelen	Conclusie		
	Opzet	Bestaan	Werking
1. Wijzigingenbeheer			
Beheersingsmaatregel	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.		
Advies	Zorg voor bewijsvoering waaruit blijkt dat wijzigingenbeheer procesmatig en procedureel wordt uitgevoerd door de gemeente Venlo		
Actie	1. Stel een wijzigingenbeheer procedure op voor de applicaties sharepoint, squit XO, zaaksysteem, en key2handhaving en toon aan dat conform die procedure wordt gewerkt.		
Voortgang (verwijzing naar document)	Actie 1: Q2: CISO		
2. Logische toegangsbeveiliging			
Beheersingsmaatregel	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.		
Advies	Zorg voor een gedocumenteerde autorisatieprocedure voor de applicaties		
Actie	1. Stel autorisatieprocedures op voor applicaties waaronder sharepoint, squit XO, zaaksysteem, en key2handhaving.		
Voortgang (verwijzing naar document)	Actie 1: Q2: CISO		
3. Beheer van kwetsbaarheden (patchmanagement)			
Beheersingsmaatregel	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.		
Advies	Documenteer voor de applicaties hoe tijdig informatie wordt verkregen over technische kwetsbaarheden en hoe daar op moet worden gereageerd (patchmanagement beleid/procedure).		

Technische en organisatorische maatregelen		Conclusie		
		Opzet	Bestaan	Werking
Actie	1. Stel een patchmanagement procedure op voor de applicaties.			
Voortgang (verwijzing naar document)	Actie 1: Q2: CISO			
4. Cryptografie				
Beheersingsmaatregel	Ter bescherming van politiegegevens behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.			
Advies	Documenteer en implementeer een beleid voor het gebruik van cryptografische beheersmaatregelen.			
Actie	1. Stel een cryptografisch beleid op en toon aan dat deze wordt toegepast voor sharepoint en de andere applicaties.			
Voortgang (verwijzing naar document)	Actie 1: Q2: CISO			
5. Vulnerability scans en Penetratietesten				
Beheersingsmaatregel	Penetratietesten en vulnerability scans worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de systemen waarin politiegegevens verwerkt worden.			
Advies	Zorg voor bewijs waaruit blijkt dat penetratietesten en vulnerabilityscans procesmatig en procedureel worden uitgevoerd voor de gemeente Venlo (Voor de gemeente Venlo is niet vastgesteld of penetratietesten en vulnerability scans procesmatig en procedureel worden uitgevoerd. De gemeente Venlo is deels zelf beheerder van de applicatie.)			
Actie	1. Toon aan op welke wijze penetratietesten en vulnerabilityscans worden uitgevoerd door de gemeente Venlo voor de applicaties.			
Voortgang (verwijzing naar document)	Actie 1: Q3: CISO			