[redacted]

Privacybeleid

Gegevensautoriteit
Definitief
Versie 1.0
10 januari 2020
Rubricering: Politie Intern

« waakzaam en dienstbaar »

Documentinformatie

Versiegeschiedenis

Versie	Versie datum	Samenvatting van de aanpassing
0.12	15-03-2019	Conceptversie
0.2	03-04-2019	Geredigeerde versie
0.3	24-04-2019	Verbeterd concept
0.32	21-05-2019	Feedback verwerkt van relevante stakeholders
0.33	08-11-2020	Vastgesteld door BBVO, uitgaande van aanpassingen ten aanzien van de Control functie
1.0	10-01-2020	Aanpassingen ten aanzien van de Control functie doorgevoerd

Distributie

Versie	Verzend datum	Naam	Afdeling / Functie
0.11	Q1 2019	5.1.2.e	Gegevensautoriteit, Verbeterprogramma Wpg en IB, Project AVG privacy
0.12	15-03-2019	5.1.2.e	Stuurgroep Wpg en IB
0.12	15-03-2019	Via 5.1.2.e	Gegegevensautoriteit
0.12	15-03-2019	Via 5.1.2.e	Stuurgroep AVG
0.31	29-04-2019	Via 5.1.2.e	Gegegevensautoriteit
0.32	10-05-2019	5.1.2.e	Gegevensautoriteit
0.32	14-05-2019	5.1.2.e	Concernaudit
0.32	14-05-2019	5.1.2.e	Functionaris voor de Gegevensbescherming
0.32	15-05-2019	Via Stuurgroep AVG	Diensten PDC
0.32	15-05-2019	Privacyplatform	Privacyfunctionarissen, Team Juridische Zaken, Privacyteam PDC, Competence Center, Dienstverlening Partners
0.32	15-05-2019	5.1.2.e	Concerncontrol
0.32	21-05-2019	5.1.2.e	Architectuurautoriteit
0.32	21-05-2019	5.1.2.e	COR werkgroep beschermingpersoonsgegevens
0.32	29-05-2019	MT IV	

0.32	07-06-2019	Driehoeksoverleg IV	
0.33	03-07-2019	5.1.2.e [redacted]	Stuurgroep Wpg en IB
0.33	03-10-2019	Hoofden Bedrijfsvoeringsoverleg	
0.33	08-11-2019	Breed Bedrijfsvoeringsoverleg	
1.0	10-01-2020	Gerrit den Uyl	Plv. vz BBVO en portefeuillehouder AVG

Inhoudsopgave

1 Inleiding

In dit privacybeleid wordt beschreven wat er ten minste moet gebeuren om de geldende wet- en regelgeving op het gebied van bescherming van persoonsgegevens na te leven.[1] Voor de politie gaat het hierbij met name om de Wet politiegegevens (Wpg) en de Algemene Verordening Gegevensbescherming (AVG)[2]. In het naleven van de Wpg en de AVG hebben alle medewerkers binnen de politie een verantwoordelijkheid. Iedere medewerker komt in zijn werk immers dagelijks in aanraking met persoonsgegevens[3]. De politie is niet alleen wapendragend maar ook informatiedragend.

De vaststelling van dit privacybeleid geeft een kader voor het uitvoeringsbeleid op het gebied van privacy. Het privacybeleid dient als een interne handleiding, waarin onder meer wordt verwezen naar uitvoeringsbeleid zoals interne protocollen en procedures die ervoor moeten zorgen dat alle risico's met betrekking tot de uitvoering van de Wpg en AVG worden onderkend en afgedekt. Daarbij wordt waar mogelijk bij bestaande structuren en werkwijzen aangesloten. Op deze manier kan de politie aantonen dat zij beleidsmatig in voldoende mate compliant is op het gebied van de privacywetgeving.

Compliant zijn in opzet, bestaan en werking van de Wpg en AVG vraagt van de politieorganisatie voldoende niveau van volwassenheid. Het model met vijf verschillende stadia van volwassenheid wordt in dit beleid verder toegelicht. Over de mate van volwassenheid wordt een ambitie uitgesproken. Met dit document heeft het korpsmanagement het privacybeleid vastgelegd, bekrachtigd en de basis gelegd voor de communicatie hierover binnen de organisatie.

1.1 Leeswijzer

De opbouw van dit document is als volgt. In hoofdstuk 2 wordt beschreven wat de visie is van de politie op het gebied van privacy. Hoofdstuk 3 bevat het doel van het privacybeleid waarna hoofdstuk 4 de strategie behandelt waarlangs deze doelstelling wordt bereikt. Hoofdstuk 5 beschrijft vervolgens welk volwassenheidsniveau wij als organisatie nastreven. In hoofdstuk 6 wordt beschreven aan welke wettelijke verplichtingen de politie moet voldoen, waar deze staan beschreven en welke verantwoordelijkheden daarbij horen. De verantwoordelijkheden, bevoegdheden, rollen en taken zijn in hoofdstuk 7 ten slotte per functie uitgewerkt. Het mandaatbesluit van de politie is daarbij leidend.

Waar in dit privacybeleid wordt verwezen naar bestaande documenten zijn deze *cursief* weergegeven. In bijlage 2 is een totaaloverzicht opgenomen, met een verwijzing naar de vindplaats.

[1] Het gaat in dit beleid dus over informationele privacy en niet over de invulling van overige privacyaspecten bij de taakuitvoering of in de bedr jfsvoering.
[2] Voor de politie kunnen naast de AVG en de Wpg ook andere wetten en regels van belang zijn. In verband met de leesbaarheid worden in dit document alleen de AVG en Wpg vermeld.
[3] Daar waar in dit beleid wordt gerefereerd aan persoonsgegevens, wordt tevens gedoeld op politiegegevens.

2 Visie op privacy

Onveranderd is de politie ‘’waakzaam en dienstbaar’’ aan de waarden van de rechtsstaat.
Ons doel als politie is Nederland veilig te houden. Om dat te kunnen doen verzamelen wij veel informatie, onder meer persoonsgegevens.

De bescherming van persoonsgegevens is een grondrecht van elke burger ten opzichte van de overheid en een waarde in de samenleving. Wij gaan dan ook conform wet- en regelgeving om met de persoonsgegevens van betrokkenen. Omdat veiligheid en burgerlijke vrijheden zoals privacy beiden belangrijk zijn, zorgen wij voor een evenwicht tussen beide belangen. Zorgvuldig omgaan met persoonsgegevens hoort bij een integere politieorganisatie.

Wij zijn transparant naar de burger over de verwerking[4] van persoonsgegevens daar waar dat kan. Als politie leggen wij verantwoording af over de verwerking van persoonsgegevens omdat dit belangrijk is voor de positie van de politie binnen de maatschappij en de acceptatie van ons gezag op straat.

Wij werken samen met partners en burgers aan veiligheid. Wij hebben een verbindende rol van wijk, web tot wereld en nemen daarin het voortouw. Wij verstrekken de noodzakelijke informatie aan andere partijen indien er sprake is van wettelijke plicht en/of een zwaarwegend algemeen belang. We zijn transparant over onze partners. We verwachten van onze samenwerkingspartners dat zij net zo zorgvuldig met persoonsgegevens omgaan als wijzelf.

Wij hebben controle over iedere gegevensverwerking die onder de verantwoordelijkheid van de politie plaatsvindt, vanaf het begin bij het verkrijgen en verzamelen van de informatie tot en met het verwijderen, overbrengen en vernietigen van informatie. Wij beveiligen de gegevens van betrokkenen en zorgen voor interne controle en toezicht. Bij nieuwe (technologische) ontwikkelingen houden we vanaf het begin rekening met de bescherming van persoonsgegevens. We verwerken niet meer persoonsgegevens dan nodig is.

Dit geldt vanzelfsprekend niet alleen voor persoonsgegevens die in het kader van de uitvoering van de politietaak worden verwerkt, maar ook voor de persoonsgegevens die, als grootste werkgever van Nederland, worden verwerkt ten behoeve van onze eigen bedrijfsvoering. Een zorgvuldige omgang met persoonsgegevens van medewerkers, leveranciers, bezoekers, sollicitanten etc. hoort ook bij een integere politieorganisatie.

[4] In de privacywetgeving heeftt het begrip “verwerking” een ruime betekenis. Een ‘verwerking’ betreft elke bewerking of elk geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd op geautomatiseerde wijze. Raadplegen, verzamelen, verstrekken en gebruiken zijn voorbeelden van verwerken.

3 Doel privacybeleid

Dit privacybeleid beoogt op organisatie- en op strategisch niveau duidelijkheid te geven over de inrichtingskeuzes rond privacy en daarmee te waarborgen dat de verwerking van persoonsgegevens op rechtmatige wijze plaatsvindt. Het privacybeleid geeft weer welke strategie het korps volgt om tot naleving van privacywetgeving te komen, welke huidige wettelijke normen daarvoor nagestreefd moeten worden en bij wie verantwoordelijkheden rond privacy zijn belegd

Aan de hand van de randvoorwaarden in het privacybeleid kunnen de verantwoordelijken in het uitvoeringsdomein een rechtmatige gegevensverwerking realiseren. Vanuit het control-/beheersdomein kan worden vastgesteld of maatregelen ter waarborging van de bescherming van persoonsgegevens afdoende zijn ingericht.

In lijn met dit algemene privacybeleid kan specifiek privacybeleid ontwikkeld worden voor processen, portefeuilles, thema's of onderdelen van de organisatie. Bovendien kan op privacyonderwerpen specifiek beleid ontwikkeld worden. De privacybeleids- en uitvoeringskaders die inmiddels door de politie zijn ontwikkeld, zijn terug te vinden in het overzicht in bijlage 2.

Doelgroepen
Vertaling van dit beleid zal plaats moeten vinden door beleidsmakers, opstellers van werkinstructies en –processen. Voor hen is dit beleid geschreven. De korpschef is als bestuurder verantwoordelijk voor privacy, hij is de zogeheten 'verwerkingsverantwoordelijke' . Deze verantwoordelijkheid is gemandateerd. Uit deze mandatering en de governance van de organisatie volgen de doelgroepen:

- de portefeuillehouder Wpg voor inrichting van de privacyfunctie[5] Wpg;
- de portefeuillehouder AVG voor inrichting van de privacyfunctie AVG;
- elke portefeuillehouder om 'oplossingen' by design en by default te laten voldoen aan privacywet- en –regelgeving;
- elke directeur van de staf korpsleiding om binnen de directie beleid by design en by default te ontwikkelen en te laten voldoen aan privacywet- en regelgeving;
- elke politiechef en de directeur PDC om binnen de eenheid, respectievelijk het PDC, privacy compliant te werken;
- de privacy- en informatiebeveiligingsprofessional voor de ondersteuning van bij de toepassing van dit beleid. Onder meer door te voorzien in uitvoeringsbeleid en richtlijnen;
- de Gegevensautoriteit voor beheer en onderhoud van dit document.

Onderhoud
Het onderhoud van dit beleid wordt vormgegeven in een cyclisch proces. Na het voorbereiden, ontwikkelen en goedkeuren volgen de fasen communicatie, implementatie en uitvoering. De uitvoering wordt geëvalueerd waarna de cyclus opnieuw start.

[5] Met de 'inrichting van de privacyfunctie' wordt gedoeld op beleid en strategie ten aaanzien van het geheel van PIOFACH factoren gericht op de bescherming van persoonsgegevens.

4 Strategie

Een strategie is de wijze waarop de doelstellingen worden bereikt. Het is - op hoofdlijnen - de manier waarop de politie het waarborgen van privacy aanpakt. Door daarbij te focussen op drie essentiële uitgangspunten wordt een systeem neergezet dat voorwaardelijk is om binnen het korps een zorgvuldige en rechtmatige omgang met persoonsgegevens te kunnen garanderen.

4.1 Uitgangspunten

Privacy is onderdeel van ieders vak

Belangrijk uitgangspunt bij de strategie is dat privacy wordt gezien als onderdeel van het werk van iedere medewerker binnen de politie. Dit houdt in dat iedere medewerker bij de uitvoering van zijn of haar werk zelf de verantwoordelijkheid heeft om ervoor te zorgen dat het werk conform de privacyregels wordt uitgevoerd. Waar mogelijk wordt de medewerker hierin ondersteund door oplossing in IV en werkprocessen, maar iedere medewerker moet ook het besef, de kennis en de middelen hebben om hiergoed invulling aan te geven. Dit geldt overigens niet alleen voor uitvoerende taken, maar ook voor leidinggevende, ontwikkelende en innoverende taken. En voor taken op het gebied van planning en control. Bij alle taken hoort privacy. Dit betekent overigens niet dat elke medewerker in de volle breedte kennis moet hebben over privacywetgeving, maar wel dat elke medewerker de voor zijn of haar werk relevante aspecten kent. Professionaliteit vraagt deskundigheid, gerelateerd aan de functie in het korps. Privacyprofessionals zoals privacyfunctionarissen zijn daarbij ondersteunend aan een organisatie die in de basis voldoende bagage heeft om zelf privacy te waarborgen.

Start van de verwerking

Een tweede uitgangspunt is dat, naast de reguliere privacybeheersing, de start van een verwerking (van persoonsgegevens) extra aandacht vereist. Privacy is onderdeel van de afweging of, en zo ja hoe, we een verwerking uitvoeren. Dit is bijvoorbeeld ook het moment om eisen te stellen aan aanbieders bij een aanbesteding. Het is tevens het moment om privacy & security by design op te nemen in de verwerking. Kortom: dit is het moment waarop er iets te kiezen valt. Een verwerking van persoonsgegevens wordt niet gestart voordat alle privacyrisico’s in beeld zijn en mitigerende maatregelen zijn genomen.

Centrale registers

Het derde uitgangspunt is gerelateerd aan het eerste. Doordat privacy onderdeel is van ieders vak, is het tot in de haarvaten van de organisatie doorgedrongen. Dit wordt beheersbaar gemaakt door de verwerkingen van persoonsgegevens centraal te registreren. Deze centrale registratie is nodig om verantwoording af te kunnen leggen, bijvoorbeeld over de afwegingen die zijn gemaakt voorafgaand aan een verwerking. Bovendien stelt het ons in staat om privacy te (be-)sturen en hierover overeenkomstig de wet transparant te zijn. Het korps voert onder meer een register van verwerkingen, van incidenten rond datalekken, een convenantenregister, een centrale registratie voor rechten van betrokkene en een registratie van verstrekkingen.

4.2 Brede borging van privacy

De borging van privacy als onderdeel van het werk vindt als volgt plaats:

1. Ontwikkelingen in de organisatie vinden plaats onder regie van een portefeuillehouder. De ontwikkelingen rond privacy vinden plaats onder regie van een portefeuillehouder AVG en een portefeuillehouder Wpg. Overige portefeuilles, programma’s, projecten, innovaties, etc. nemen privacy, met in achtneming van dit privacybeleid, mee in hun ontwikkeling. Dit kan op aangeven van de portefeuillehouder AVG of Wpg plaatsvinden.
2. De beheersing van privacy in de uitvoering volgt de bestaande beheersstructuur van het korps (dit omvat onder andere sturing, planning en control, audit, opleidingen, communicatie, etc.)

Voor zowel de ontwikkeling als de uitvoering wordt gebruik gemaakt van de privacybaseline van het Centrum Informatiebeveiliging en Privacybescherming[6]. Deze privacybaseline heeft de principes voor privacybeleid, -uitvoering en -control vertaald naar normen die gehaald moeten worden om aan de wet te voldoen. In aanvulling op de baseline wordt een risicogebaseerde aanpak gehanteerd. In een cyclisch proces worden privacyrisico's geïdentificeerd en mitigerende maatregelen genomen. Deze kunnen zowel een nieuwe ontwikkeling als een verbetering in de beheersing betreffen.

Voor de *borging* en de *ontwikkeling* van privacy heeft de organisatie specifieke privacyfuncties vormgegeven. Deze staan beschreven in hoofdstuk 7. De specifieke privacyfuncties zijn er voor:
1. beleid, instructies en sjablonen, voor de juiste toepassing van privacy;
2. (systeem-) toezicht op de naleving van privacy;
3. specialistische privacytaken zoals rechten van betrokkene;
4. advisering.

4.3 De start van een verwerking

Belangrijk bij privacy is dat de juiste afweging heeft plaatsgevonden tussen de inbreuk die wordt gepleegd op de persoonlijke levenssfeer van een betrokkene, de wettelijke grondslagen en het doel waarvoor deze verwerking plaats gaat vinden. Deze afweging vindt plaats voorafgaand aan de start van een verwerking en wordt zo geregistreerd dat de organisatie zich hierover (eenvoudig) kan verantwoorden (ook ongevraagd: informatieplicht en transparantie). Voor de juiste afweging is voldoende privacykennis onontbeerlijk. Voor de start van een verwerking wordt[7]:

1. de privacyimpact (en bescherming van persoonsgegevens) van een verwerking ingeschat;
2. bij een hoog risico een Gegevensbeschermingseffectbeoordeling (GEB) uitgevoerd;
3. de GEB toegestuurd aan de functionaris voor gegevensbescherming. Zo nodig wordt de Autoriteit Persoonsgegevens voorafgaand geraadpleegd;
4. privacy & security by design toegepast[8].

Onderdeel van bovenstaande activiteiten omvat een beschrijving van de wijze waarop wordt voldaan aan de wettelijke vereisten. Deze staan beschreven in hoofdstuk 6.

Iedere verwerkingsverantwoordelijke dient bovenstaande stappen te doorlopen voorafgaand aan de verwerking. Zonder het doorlopen van deze stappen kan de verwerking niet starten. Ook bij het onvoldoende afdekken van de privacyrisico's (volgend uit de GEB) kan een verwerking niet starten.

Bovenstaande wordt geborgd door:
1. aan iedere verwerking een verantwoordelijke op een passend niveau in het korps te koppelen;
2. besluitvormingsprocessen zo in te richten dat verwerkingen alleen wanneer zij met een positief resultaat bovenstaande stappen hebben doorlopen, doorgang kunnen vinden;
3. verwerkingen vast te leggen in een register en alle afspraken en convenanten in een register op te nemen ter invulling van de verantwoordingsplicht en ten behoeve van de privacybeheersing en transparantie;
4. privacy & security by design te borgen in ontwikkelactiviteiten in de organisatie. Het betreft hier onder andere portefeuilles en voortbrengingsprocessen van de Dienst IM en de Dienst ICT. Extra focus krijgen architectuur en privacy als onderdeel van de kwaliteitsbewaking in programma's en projecten;
5. bij de verwerving van producten en diensten de bescherming van persoons- en politiegegevens mee te nemen;

---

[6] Privacybaseline is terug te vinden op https://www.noraonline.nl/wiki/De_Privacy_Baseline. Op sommige punten wordt afgeweken van de baseline omdat de Wpg dat op onderdelen vereist. Een andere reden is dat verschillende elementen in specifiek beleid worden uitgewerkt. Dit geldt voor risicomanagement, het control- en beheersdomein en het uitvoeringsdomein. Uiteindelijk komen alle elementen uit de baseline aan bod.
[7] De start van een verwerking betreft het ontwerpen/opzetten van een bedrijfsproces of systeem waarin persoonsgegeven worden verwerkt. Het betreft niet het starten van bijvoorbeeld een zaak of onderzoek binnen een bestaand bedrijfsproces of systeem.
[8] Zie uitvoeringskader Privacy & Security by Design

6. ondersteuning van de lijn door privacyprofessionals;
7. toezicht op dit alles door de functionaris voor gegevensbescherming.

Bovenstaande geldt voor iedere nieuwe verwerking of iedere wijziging in een verwerking. Indien een verwerking nog niet voldoet geldt dat het bovenstaande alsnog uitgevoerd moet worden.

5 Privacyvolwassenheid

Voor de privacyvolwassenheid gebruikt de politie het volwassenheidsmodel van het Centrum voor Informatiebeveiliging en Privacybescherming[9]. Dit model sluit aan op de privacybaseline (zie hoofdstuk 4). Voor de Wpg en andere sectorspecifieke wetten en verordeningen is de baseline aangepast. In lijn hiermee wordt ook het volwassenheidsmodel aangepast.

In het privacyvolwassenheidsmodel is per (wettelijke) norm beschreven waaraan voldaan moet zijn om een bepaald volwassenheidsniveau te bereiken. Het niveau geeft daarbij de mate aan, waarin de organisatie van privacy is gesystematiseerd en geïnternaliseerd in de politieorgansatie.

Verplichting tot privacy compliance
Met het vaststellen van dit privacybeleid committeren de korpsleiding en het korpsmanagementteam zich aan het bereiken van ten minste volwassenheidsniveau 3.
In het derde niveau van volwassenheid[10] is er sprake van compliance aan privacy wet- en regelgeving. Vanuit de gedachte 'basis op orde' is dit het niveau dat de politie de komende tijd wil gaan bereiken. Dit gebeurt op de in de strategie geschetste wijze (zie hoofdstuk 4). De korpschef, de politiechefs, de directeur PDC en de lijnmanager hebben ieder een eigen verantwoordelijkheid voor het opstellen van een roadmap privacyvolwassenheid. In de roadmap wordt vastgelegd welke stappen op welk moment verwezenlijkt gaan worden om het gewenst ambitieniveau te bereiken. Voor de roadmap worden de volgende uitgangspunten gehanteerd: Nieuwe diensten, processen, applicaties, etc. worden direct compliant opgeleverd. Verbetering van bestaande dienst, processen, applicaties, etc. resulteert op termijn in een compliant oplossing (volgens een stappenplan). Dienst, processen, applicaties, etc. die uitgefaseerd worden, volgen een saneerplan waarin rekening is gehouden met o.a. het privacyrisico.

Op niveau 3 verwerkt de politie gegevens, waarbij keuzes zijn en worden gemaakt op basis van operationeel beleid, richtlijnen en werkinstructies op organisatieniveau. Het beleid is formeel vastgesteld op organisatieniveau en daarmee bekrachtigd als beleid voor de gehele politieorganisatie. De vereisten vanuit de organisatie zijn ook vertaald naar de inrichting van de context, de systemen en de beheerprocessen. De politieorganisatie leert bedrijfsbreed, omdat er een systematische samenhang bestaat tussen de uitvoerende onderdelen, beleidsonderdelen en controleonderdelen op alle niveaus. Er is structurele evaluatie van en rapportage over de gegevensverwerking (en beveiliging van gegevens) naar het hogere management, wat tot aanpassing van het organisatiebrede beleid kan leiden. Er bestaat sturing op de naleving van het beleid, richtlijnen en (werk)instructies. De leiding is betrokken bij de handhaving van het beleid en de uitvoering, waarbij gerapporteerd wordt ondersteund door controlemiddelen en informatie. Dit leidt tot een lerend proces op alle niveaus.

[9] Het privacyvolwassenheidsmodel is terug te vinden op https://www.cip-overheid.nl/wp-content/uploads/2018/01/20171102-Privacy-Volwassenheidsmodel-v3_0_9.pdf
[10] Detailbeschrijving per volwassenheidsniveau staat in bijlage 1

6 Wettelijke kaders privacy (AVG en Wpg)

Om privacy compliant te zijn, moet de politie aan de wettelijke verplichtingen voldoen. In de privacybaseline van het Centrum voor Informatiebeveiliging en Privacy zijn de wettelijke verplichtingen uitgewerkt in normen (zie hoofdstuk 4). In dit hoofdstuk wordt, door per norm aan te geven hoe deze door de politie wordt toegepast, een vertaling gemaakt van de wet naar uitvoering in de organisatie.

De tabellen in dit hoofdstuk geven het volgende weer:
- De norm zoals beschreven in de privacy baseline;
- welk beleid, kader en richtlijnen van toepassing zijn;
- welke partijen een rol hebben in de verplichting.

Waar toepasbaar beleid (of andere documenten) beschikbaar is, dan is in bijlage 2 een hyperlink ingevoegd. Het kan ook zijn dat specifiek beleid in ontwikkeling is.

Start van de verwerking	
Norm	Beschreven is hoe gewaarborgd wordt dat verantwoordelijken vooraf aantoonbaar maatregelen hebben genomen door het toepassen van privacy by design, het uitvoeren van GEB's en het gebruik van standaardinstellingen.
Beleid, kaders en richtlijnen	• In het *Uitvoeringskader privacy & security by design* is vastgelegd op welke wijze invulling moet worden gegeven aan de beginselen van privacy by design en het gebruik van standaardinstellingen. De principes die daar nader op ingaan zijn 'PDCA-cyclus' en 'Privacy by Default'. • In het *Beleidskader registerplicht en GEB* is vastgelegd wanneer een GEB moet worden uitgevoerd, wie hiertoe het initiatief moet nemen, wie bij de uitvoering van de GEB betrokken moeten worden en wie een beslissing moet nemen over de te nemen mitigerende maatregelen.
Verantwoor-delijken	• De verantwoordelijke voor de verwerking (bijv. politiechef, portefeuillehouder, sectorhoofd) zorgt voor de uitvoering van het specifieke beleid. • Elke medewerker werkt met de juiste procedures bij het uitvoeren van het specifieke beleid. • De Gegevensautoriteit draagt zorg voor de (door)ontwikkeling van het specifieke beleid met betrekking tot privacy by design, het uitvoeren van GEB's en het gebruik van standaardinstellingen.

Doelbinding gegevensverwerking	
Norm	AVG Beschreven is hoe gewaarborgd wordt dat persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en dat de gegevens niet op een met die doeleinden onverenigbare wijze worden verwerkt. Wpg Beschreven is hoe gewaarborgd wordt dat politiegegevens slechts worden verwerkt voor zover dat noodzakelijk is voor de bij of krachtens de Wpg geformuleerde gerechtvaardigde doeleinden en slechts worden verwerkt voor een ander doel voor zover de Wpg daar uitdrukkelijk in voorziet en de verwerking voor dat andere doel noodzakelijk is en in verhouding staat tot dat doel.
Beleid, kaders en richtlijnen	• In het *Uitvoeringskader privacy & security by design* is beschreven op welke wijze invulling moet worden gegeven aan privacywetgeving, waaronder het begrip doelbinding. • In het *Beleidskader registerplicht en GEB* is vastgelegd wanneer een GEB moet worden uitgevoerd, wie hiertoe het initiatief moet nemen, wie bij de uitvoering van de GEB betrokken moeten worden en wie een beslissing moet nemen over de te nemen mitigerende maatregelen.
Verantwoor-delijken	• De verantwoordelijke voor de verwerking (bijv. politiechef, portefeuillehouder, sectorhoofd) zorgt voor de uitvoering van het specifieke beleid.

Doelbinding gegevensverwerking	
	• Elke medewerker werkt met de juiste procedures bij het uitvoeren van het specifieke beleid. • De Gegevensautoriteit draagt zorg voor de (door)ontwikkeling van het specifieke beleid met betrekking tot privacy by design en het bijhouden van een verwerkingsregister, inclusief het vastleggen van een beschrijving van de verwerkingsdoeleinden.

Kwaliteitsmanagement	
Norm	Beschreven is hoe gewaarborgd wordt dat de persoonsgegevens, gelet op de doeleinden waarvoor zij worden verwerkt juist zijn. Mocht dit niet het geval zijn, dan moeten alle redelijke maatregelen worden genomen om de persoonsgegevens die onjuist zijn, onverwijld te wissen of te rectificeren.
Beleid, kaders en richtlijnen	In het *Uitvoeringskader privacy & security by design* is beschreven op welke wijze invulling moet worden gegeven aan privacywetgeving, waaronder de eisen rond de kwaliteit van gegevens. De principes die daar nader op ingaan zijn 'eenmalige vastlegging', 'metagegevens' en 'kwaliteitszorg'.
Verantwoor-delijken	• De verantwoordelijke voor de verwerking (bijv. politiechef, portefeuillehouder, sectorhoofd) zorgt voor de uitvoering van het specifieke beleid, bijvoorbeeld door relevante aspecten te verwerken in richtlijnen of werkinstructies. • Elke medewerker werkt met de juiste procedures bij het uitvoeren van het specifieke beleid. • De Gegevensautoriteit draagt zorg voor de (door)ontwikkeling van het specifieke beleid met betrekking tot privacy by design.

Minimale gegevensverwerking	
Norm	Beschreven is hoe gewaarborgd wordt dat de verwerking toereikend, ter zake dienend en beperkt s tot "minimale gegevensverwerking"; tot wat noodzakelijk is voor de doeleinden waarvoor de gegevens worden verwerkt.
Beleid, kaders en richtlijnen	In het *Uitvoeringskader privacy & security by design* is beschreven op welke wijze invulling moet worden gegeven aan privacywetgeving, waaronder de eis van minimale gegevensverwerking. Het principe dat daar nader op ingaat 'is 'privacy by default'.
Verantwoor-delijken	• De verantwoordelijke voor de verwerking (bijv. politiechef, portefeuillehouder, sectorhoofd) zorgt voor de uitvoering van het specifiek beleid, bijvoorbeeld door relevante aspecten te verwerken in richtlijnen of werkinstructies.. • Elke medewerker werkt met de juiste procedures bij het uitvoeren van het specifieke beleid. • De Gegevensautoriteit draagt zorg voor de (door)ontwikkeling van het specifieke beleid met betrekking tot privacy by design.

Beveiliging van de verwerking van persoonsgegevens	
Norm	Beschreven is hoe gewaarborgd wordt dat passende technische en organisatorische beveiligingsmaatregelen worden getroffen, zodat duidelijk is hoe de verwerking wordt gewaarborgd en hoe de persoonsgegevens onder meer worden beschermd tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.
Beleid, kaders en richtlijnen	• In het *Informatiebeveiligingsbeleid* is beschreven op welke wijze is gewaarborgd dat passende en organisatorische beveiligingsmaatregelen worden getroffen. • In het *Uitvoeringskader privacy & security by design* is beschreven op welke wijze invulling moet worden gegeven aan privacywetgeving, waaronder beveiliging van persoonsgegevens. De principes die daar nader op ingaan zijn 'autorisatie' en 'informatiebeveiliging'.
Verantwoor-delijken	• De verantwoordelijke voor de verwerking (bijv. politiechef, portefeuillehouder, sectorhoofd) zorgt voor de uitvoering van het specifiek beleid. • Elke medewerker werkt met de juiste procedures bij het uitvoeren van het specifieke beleid.

Beveiliging van de verwerking van persoonsgegevens	
	• De CISO draagt zorg voor de (door)ontwikkeling van het Informatiebeveiligingsbeleid. • De CISO draagt zorg voor de (door)ontwikkeling van het specifieke beleid met betrekking tot privacy & security by design, voor zover het eisen rond de beveiliging van persoonsgegevens betreft.

Rechten van de betrokkene	
Norm	Beschreven is hoe gewaarborgd wordt dat de persoonsgegevens op een wijze worden verwerkt die voor het publiek en de betrokkene transparant is en het de betrokkene mogelijk maakt zijn rechten uit te oefenen. Hierbij is specifiek aandacht voor de bescherming van kinderen.
Beleid, kaders en richtlijnen	• In specifiek beleid met betrekking tot informatieverstrekking aan betrokkene wordt beschreven op welke wijze invulling wordt gegeven aan de algemene en specifieke informatieplicht, waaronder de publicatie van een privacy statement. • In de *Handleiding rechten van betrokkene* wordt vastgelegd op welke wijze om moet worden gegaan met verzoeken in het kader van de rechten van betrokkenen.
Verantwoor-delijken	• De verantwoordelijke voor de verwerking (bijv. politiechef, portefeuillehouder, sectorhoofd) zorgt voor de uitvoering van het beleid rond de specifieke informatieplicht. • De privacydeskmedewerker voert de werkzaamheden met betrekking tot de verzoeken van de rechten van betrokkene uit overeenkomstig de *Handleiding rechten van betrokkene*. • De Gegevensautoriteit draagt zorg voor de ontwikkeling van het specifieke beleid met betrekking tot de algemene en specifieke informatieplicht, zoals de *Handleiding rechten van betrokkene*, en voor de publicatie van het algemene privacystatement.

Bewaren van persoonsgegevens	
Norm	Beschreven is hoe gewaarborgd wordt dat persoonsgegevens niet langer worden bewaard dan waarvoor zij worden verwerkt noodzakelijk is en in welke vorm de opslag moet plaatsvinden zodat na deze periode de betrokkenen niet langer zijn te identificeren.
Beleid, kaders en richtlijnen	• In het *Uitvoeringskader privacy & security by design* is beschreven op welke wijze invulling moet worden gegeven aan privacywetgeving, waaronder de bewaartermijnen. Het principe dat hier nader op ingaat is 'bewaren' en 'vernietigen'. • In het specifieke beleid *Bewaartermijnen* wordt beschreven welke wettelijke bepalingen in dit kader relevant zijn, hoe ze zich tot elkaar verhouden en hoe invulling moet worden gegeven aan de eisen rond bewaartermijnen. • In de *Selectielijst* zijn de bewaartermijnen van archiefbescheiden van de politie beschreven.
Verantwoor-delijken	• De verantwoordelijke voor de verwerking (bijv. politiechef, portefeuillehouder, sectorhoofd) zorgt voor de uitvoering van het beleid rond bewaartermijnen. • De Gegevensautoriteit draagt zorg voor de (door)ontwikkeling van het specifieke beleid met betrekking tot privacy by design en het specifieke beleid met betrekking tot bewaartermijnen.

Doorgifte of verstrekking van persoonsgegevens	
Norm	Beschreven is hoe gewaarborgd wordt dat persoonsgegevens slechts worden doorgegeven, verstrekt of ter beschikking gesteld[11] wanneer daar een grondslag voor is en formeel afdoende garanties zijn vastgelegd zodat aangetoond kan worden dat ook bij de doorgifte, verstrekking of terbeschikkingstelling aan de AVG of Wpg wordt voldaan en wat in verwerkersovereenkomsten en samenwerkingsovereenkomsten moet worden vastgelegd.

[11] 'Ter beschikking stellen' is alleen relevant voor verwerkingen op grond van de Wpg, niet voor de AVG.

Doorgifte of verstrekking van persoonsgegevens	
Beleid, kaders en richtlijnen	• In het *Uitvoeringskader privacy & security by design* is beschreven op welke wijze invulling moet worden gegeven aan privacywetgeving, waaronder het het verstrekken van persoonsgegevens. Het principe dat hier nader op ingaat is 'doelbinding'. • In het *Beleidskader registerplicht en GEB* wordt onder meer beschreven op welke wijze moet worden bepaald en vastgelegd wie de ontvangers van de persoonsgegevens zijn. • De *Verstrekkingenwijzer* geeft een overzicht van de personen en instanties waar politiegegevens aan verstrekt mogen worden. • In specifiek beleid met betrekking tot verwerkersovereenkomsten wordt beschreven wanneer een verwerkersovereenkomst moet worden aangegaan en welke elementen daar minimaal in moeten zijn opgenomen. Ook wordt een model beschikbaar gesteld. • In specifiek beleid met betrekking tot samenwerkingsverbanden wordt beschreven wanneer aan een samenwerkingsverband kan worden deelgenomen en welke elementen minimaal in een convenant en een artikel 20-beslissing moeten zijn opgenomen. Ook worden modellen beschikbaar gesteld.
Verantwoordelijken	• De verantwoordelijke voor de verwerking (bijv. politiechef, portefeuillehouder, sectorhoofd) zorgt voor de uitvoering van het beleid rond de doorgifte of verstrekking van persoonsgegevens. • Elke medewerker werkt met de juiste procedures bij het uitvoeren van het specifieke beleid. • De Gegevensautoriteit draagt zorg voor de ontwikkeling van het specifieke beleid met betrekking tot het bijhouden van een verwerkingsregister, waaronder het bepalen en vastleggen van de ontvangers van persoonsgegevens. De Gegevensautoriteit draagt ook zorg voor de ontwikkeling van het specifieke beleid met betrekking tot verwerkersovereenkomsten en samenwerkingsverbanden.

Register en verwerkingsactiviteiten	
Norm	Beschreven is hoe gewaarborgd wordt hoe verantwoordelijken aantonen dat gedurende en na de verwerking de verwerking ten aanzien van de betrokkene behoorlijk is en hoe dit door middel van het bijhouden van een register en een dossier kan worden aangetoond.
Beleid, kaders en richtlijnen	In het *Beleidskader registerplicht en GEB* wordt beschreven op welke wijze invulling wordt gegeven aan het vastleggen van verwerkingsactiviteiten in een register ten behoeve van de verantwoordingsplicht.
Verantwoordelijken	• De verantwoordelijke voor de verwerking (bijv. politiechef, portefeuillehouder, sectorhoofd) zorgt voor de uitvoering van het beleid rond het bijhouden van een verwerkingsregister. • Elke medewerker werkt volgens de juiste procedures bij het uitvoeren van het specifieke beleid. • De Gegevensautoriteit draagt zorg voor de ontwikkeling van het specifieke beleid met betrekking tot het bijhouden van een verwerkingsregister.

Meldplicht datalekken	
Norm	Beschreven is hoe gewaarborgd wordt dat bij een inbreuk in verband met persoonsgegevens (datalek) de betrokkenen en de AP worden geïnformeerd als deze inbreuk waarschijnlijk een risico nhoudt voor de rechten en / of vrijheden van natuurlijke personen.
Beleid, kaders en richtlijnen	• In de *Procesbeschrijving meldplicht datalekken* is beschreven op welke wijze is gewaarborgd dat bij een inbreuk in verband met persoonsgegevens de betrokkenen en de AP worden geïnformeerd en het incident wordt vastgelegd in een register. • In het *Uitvoeringskader privacy & security by design* is beschreven op welke wijze invulling moet worden gegeven aan privacywetgeving, waaronder het begrip meldplicht datalekken. Het principe dat hier nader op ingaat is 'verantwoording'
Verantwoordelijken	• De verantwoordelijke voor de verwerking (bijv. politiechef, portefeuillehouder, sectorhoofd) zorgt voor de uitvoering van het beleid rond het melden van datalekken.

Meldplicht datalekken	
	• Elke medewerker werkt met de juiste procedures bij het uitvoeren van het specifieke beleid en is verantwoordelijk voor het (intern) melden van datalekken. • De CISO draagt zorg voor de (door)ontwikkeling van de *Procesbeschrijving meldplicht datalekken*.

Logging	
Norm	Beschreven is hoe gewaarborgd wordt dat bepaalde handelingen met betrekking tot persoonsgegevens worden vastgelegd zodat de rechtmatigheid van de gegevensverwerking kan worden aangetoond, een en ander ter waarborging van de integriteit en de beveiliging van persoonsgegevens.
Beleid, kaders en richtlijnen	• In het *Beleidskader logging* is beschreven op welke wijze invulling moet worden gegeven aan de verplichtingen rond logging. • In het *Uitvoeringskader privacy & security by design* is beschreven op welke wijze invulling moet worden gegeven aan privacywetgeving, waaronder het begrip logging. Het principe dat hier nader op ingaat is 'verantwoording'.
Verantwoor-delijken	• De verantwoordelijke voor de verwerking (bijv. politiechef, portefeuillehouder, sectorhoofd) zorgt voor de uitvoering van het beleid rond logging. • De CISO draagt zorg voor de ontwikkeling van specifiek beleid rond de vastlegging, monitoring van en toegang tot loggegevens.

Autorisaties	
Norm	Beschreven is hoe gewaarborgd wordt dat een systeem van autorisaties wordt onderhouden dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid, zodat persoonsgegevens slechts worden verwerkt door personen die daartoe door de verwerkingsverantwoordelijke zijn geautoriseerd en voor zover de autorisatie strekt.
Beleid, kaders en richtlijnen	• In het *Autorisatiebeleid* is beschreven op welke wijze wordt gewaarborgd dat een systeem van autorisaties wordt onderhouden dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid. • In het *Uitvoeringskader privacy & security by design* is beschreven op welke wijze invulling moet worden gegeven aan privacywetgeving, waaronder het begrip autorisatie. Het principe dat hier nader op ingaat is 'autorisatie'
Verantwoor-delijken	• De verantwoordelijke voor de verwerking (bijv. politiechef, portefeuillehouder, sectorhoofd) zorgt voor de uitvoering van het beleid rond autorisaties. • Elke medewerker, in het bijzonder de leidinggevende in verband met zijn rol in de Autorisatietool leidinggevenden (ATL), werkt met de juiste procedures bij het uitvoeren van het Autorisatiebeleid. • De CISO draagt zorg voor de ontwikkeling van specifiek beleid rond autoriseren.

Intern toezicht	
Norm	Beschreven is hoe gewaarborgd wordt dat intern toezicht op de rechtmatige en zorgvuldige verwerking van persoonsgegevens plaatsvindt.
Beleid, kaders en richtlijnen	• In een intern auditplan wordt vastgelegd wat het doel van de interne audit is, wat de inhoud/het object is, wat de doorlooptijd is, wat de onderzoeksinstrumenten zijn, de wijze waarop en de termijn waarbinnen wordt gerapporteerd, op welke wijze de verzamelde informatie beveiligd is, de geheimhoudingsplicht en de aanbieding en verspreidingskring van de rapportage.[12]

[12] Artikel 3, lid 4 van de Regeling periodieke audit politiegegevens

Intern toezicht	
	• In een toezichtkalender wordt jaarlijks beschreven welke toezichtsactiviteiten plaats vinden.
Verantwoor-delijken	• Concernaudit draagt zorg voor de ontwikkeling en uitvoering van het intern auditplan. • De functionaris voor gegevensbescherming en de privacyfunctionarissen dragen zorg voor een jaarlijkse toezichtkalender en voeren het toezicht uit.

Documentatieplicht (Wpg)	
Norm	Beschreven is hoe gewaarborgd wordt dat documentatiegegevens overeenkomstig artikel 32 van de Wpg worden vastgelegd en de privacyfunctionaris daar een overzicht van heeft.
Beleid, kaders en richtlijnen	In specifiek beleid met betrekking tot het schriftelijk vastleggen van bepaalde gegevens wordt beschreven op welke wijze invulling wordt gegeven aan deze documentatieplicht.
Verantwoor-delijken	• De verantwoordelijke voor de verwerking (bijv. politiechef, portefeuillehouder, sectorhoofd) zorgt voor de uitvoering van het beleid rond het vastleggen van gegevens op grond van de documentatieplicht. • Elke medewerker werkt met de juiste procedures bij het uitvoeren van het specifieke beleid. • De privacyfunctionaris houdt een overzicht bij van de gegevens die op grond van de documentatieplicht worden vastgelegd. • De Gegevensautoriteit draagt zorg voor de ontwikkeling van het specifieke beleid met betrekking tot het vastleggen van gegevens op grond van de documentatieplicht.

7 Privacymanagement

7.1 Governancestructuur politie

Het privacybeleid wordt ingebed in de governancestructuur van de politie. Dit betekent dat het privacybeleid aansluit bij de vastgestelde hoofdstructuur voor sturing en besturing, verdeling van verantwoordelijkheden, rol van de medezeggenschap, planning en control cyclus, controlorganisatie, auditfunctie en toezichtstructuur[13].

De korpschef is verantwoordelijk voor de rechtmatige en zorgvuldige verwerking van persoonsgegevens en opzet, bestaan en werking van de privacyorganisatie binnen de politie. Deze verantwoordelijkheid is via het mandaatbesluit gemandateerd. Een lid van de korpsleiding heeft de portefeuille bedrijfsvoering, waar een rechtmatige en zorgvuldige verwerking van persoonsgegevens in de bedrijfsvoering aan is gekoppeld. Een ander lid van de korpsleiding heeft de portefeuille operatiën, waar een rechtmatige en zorgvuldige verwerking van persoonsgegevens bij de operationele politietaakuitvoering aan is gekoppeld.

De inrichting van het korps bestaat uit vier organisatieniveaus, via die niveaus loopt de lijnsturing. Ten aanzien van de operationele taakuitvoering wordt onderscheid gemaakt tussen korpsniveau, eenheidsniveau (politiechefs), districts- en sectorniveau en teamniveau. Ten aanzien van de bedrijfsvoering gaat het om korpsniveau, directieniveau (directeur PDC), dienstniveau en afdelingsniveau.

Bovengenoemde ‘lijn’ heeft voortdurend actueel zicht op de stand van zaken van zijn onderdeel van de organisatie, het verloop van de werkprocessen, de voortgang in het realiseren van de resultaten, effecten en risico’s. De lijn legt verantwoording af over de resultaten en de wijze waarop die zijn behaald.

Daarnaast kunnen leden die deelnemen aan het korpsmanagementteamoverleg[14] (KMTO) voor specifieke onderwerpen op het gebied van de bedrijfsvoering en de taakuitvoering worden aangewezen als landelijk portefeuillehouder. De portefeuilles zijn gericht op planvorming en monitoring van de uitvoering. De landelijk portefeuillehouders zijn verantwoordelijk voor beleidsvorming rond de portefeuille en voorbereiding van besluitvorming inclusief impactanalyse op de eenheden en het PDC. De landelijk portefeuillehouder zorgt dat bij de beleidsvorming in opzet wordt voldaan aan een rechtmatige en zorgvuldige verwerking van persoonsgegevens. Implementatie van de voorstellen ligt bij de lijn.[15]

Het ontwikkelen van landelijk beleid en veranderkracht met betrekking tot de bescherming van persoonsgegevens is geborgd binnen een landelijke portefeuille AVG (bedrijfsvoering, korpscheftaken en vreemdelingentaken) en een landelijke portefeuille Wpg.

7.2 Verantwoordelijkheden en bevoegdheden privacy

In deze paragraaf worden de verantwoordelijkheden en bevoegdheden die volgen uit de AVG, de Wpg, het landelijke mandaatbesluit[16] en de governancestructuur uitgewerkt. Daarbij wordt benadrukt dat het mandaatbesluit leidend is en onderstaande een weerslag is van de belangrijkste consequenties daarvan. Dit laat onverlet dat de algehele verantwoordelijkheid om conform privacywet- en regelgeving te werken via bovengenoemde governancestructuur is belegd.

Het is mogelijk dat sommige bevoegheden binnen een organisatieonderdeel zijn ondergemandateerd, zoals bijvoorbeeld de bevoegdheid om beslissingen op grond van artikel 20 van de Wpg te nemen. Dergelijk regionale verschillen, zijn niet in dit privacybeleid opgenomen.

---

[13] Zie Governance notitie versie 1.0, p.12.
[14] Deelnemers aan het KMTO zijn: de leden van de korpsleiding, de politiechefs, de directeur van de Politieacademie, de directeur van het Politiedienstencentrum en de korpscontroller.
[15] Zie het KMT-besluit Commissies en Portefeuilles van 6 december 2017 voor een verdere toelichting op de rol van landel jk portefeuillehouder.
[16] Mandaatbesluit politie september 2017

Verwerkersrol

Voor sommige gegevenswerkingen is de korpschef geen verwerkingsverantwoordelijke maar verwerker[17]. Dat betekent dat gegevens ten behoeve van een andere verwerkingsverantwoordelijke worden verwerkt. Voorbeelden daarvan zijn gegevens die ten behoeve van de Politieacademie worden verwerkt, of ten behoeve van partners zoals de Rijksrecherche, de KMar of de bijzondere opsporingsdiensten, maar ook ten behoeve van partners in de strafrecht- of vreemdelingenketen. Een voorbeeld hiervan is de Basis Voorziening Vreemdelingen (BVV). Gerealiseerd moet worden dat de verantwoordelijkheden die voortvloeien uit de verwerkersrol van de korpschef de governancestructuur volgen.
Ook ten aanzien van deze rol wordt specifiek uitvoeringsbeleid ontwikkeld.

Functie	Verantwoordelijkheden en bevoegdheden
Korpschef	1. Is verwerkingsverantwoordelijke dan wel verwerker ten aanzien van persoonsgegevens die door de politie onder de AVG en Wpg worden verwerkt. 2. Benoemt een functionaris voor gegevensbescherming, bedoeld in artikel 37 van de AVG en artikel 36 van de Wpg. 3. Legt de bij of krachtens artikel 13, vierde lid Wpg bepaalde gegevens met betrekking tot de verwerking van politiegegevens ter ondersteuning van de politietaak, bedoeld in artikel 13, leden 1, 2 en 3, vast. 4. Laat periodiek de naleving van de bij of krachtens de Wpg gegeven regels controleren door periodiek privacyaudits als bedoeld in artikel 2 van de *Regeling periodieke audit politiegegevens* te laten uitvoeren. 5. Stelt het privacybeleid vast.

Functie	Verantwoordelijkheden en bevoegdheden
Politiechef	1. Benoemt de privacyfunctionaris(sen) voor zijn eenheid. 2. Laat periodiek de naleving van de bij of krachtens de Wpg gegeven regels controleren door periodiek interne privacyaudits als bedoeld in artikel 3 van de *Regeling periodieke audits politiegegevens* te laten uitvoeren. 3. Neemt beslissingen over incidentele en structurele verstrekkingen (in het kader van samenwerkingsverbanden) op grond van art. 19 en 20 van de Wpg. 4. Wijst op grond van artikel 6, lid 7 van de Wpg bevoegd functionarissen binnen zijn eenheid aan.

Functie	Verantwoordelijkheden en bevoegdheden
Directeur	1. De directeuren korpsstaf en operatiën benoemen voor hun directie de privacyfunctionaris op grond van artikel 34 van de Wpg. 2. De directeur PDC verleent geen ondermandaat voor het benoemen van een privacyfunctionaris op grond van artikel 34 van de Wpg, tenzij aan de diensthoofden van het PDC dan wel het hoofd bedrijfsvoering van de Politieacademie.

Functie	Verantwoordelijkheden en bevoegdheden
Lijnmanager	1. Is binnen het geheel aan kaders verantwoordelijk voor een rechtmatige en zorgvuldige verwerking van persoonsgegevens binnen zijn organisatieonderdeel en voor de opzet, bestaan en werking van de organisatie daarvan. 2. Beslist over het toekennen, wijzigen en intrekken van autorisaties van zijn medewerkers.

[17] Artikel 28 AVG en artikel 6c Wpg

Functie	Verantwoordelijkheden en bevoegdheden
Functionaris voor gegevensbescherming	De functionaris voor gegevensbescherming is beheersmatig onderdeel van het team Veiligheid, Integriteit en Klachten, als onderdeel van de Korpsstaf. Er is geen sprake van een ijnverantwoordelijkheid, hij rapporteert rechtstreeks aan de korpschef. De functionaris voor gegevensbescherming richt zich vooral op het uitoefenen van toezicht op de gegevenswerking van de politie. Zijn positie, taken en bevoegdheden zijn vastgelegd in artikel 37 tot en met 39 van de AVG en artikel 36 van de Wpg.[18] 1. Houdt intern toezicht op de naleving van de AVG en Wpg in de organisatie en voert in het kader daarvan ook onderzoek uit. 2. Signaleert en adviseert intern op het gebied van privacy om in de organisatie naleving van de privacywetgeving te borgen. 3. Rapporteert aan de korpschef over de bevindingen over de naleving van de AVG en de Wpg in de organisatie. 4. Verstrekt desgevraagd advies met betrekking tot de gegevensbeschermingseffectbeoordeling en ziet toe op de uitvoering daarvan. 5. Treedt op als contactpunt voor de Autoriteit Persoonsgegevens voor zaken omtrent de verwerking van persoonsgegevens. 6. Stelt jaarlijks een verslag op met de bevindingen over de naleving van de AVG en de Wpg in de organisatie.

Functie	Verantwoordelijkheden en bevoegdheden
Privacy-functionaris	1. Signaleert en adviseert op strategisch, tactisch en operationeel niveau over de naleving van de AVG en de Wpg binnen de eenheid of het PDC. 2. Adviseert over de naleving van de AVG en de Wpg op landelijke thema's voor zover het aan de eenheid of het PDC gemandateerde portefeuilles betreft. 3. Houdt toezicht op de naleving van de AVG en de Wpg binnen de eenheid of het PDC. 4. Houdt een overzicht bij van de schriftelijke vastlegging van gegevens als bedoeld in artikel 32, tweede lid van de Wpg. 5. Stelt jaarlijks een verslag op van de bevindingen over de naleving van de AVG en de Wpg in zijn eenheid, alsmede de landelijke portefeuille van de eenheid of het PDC.

Functie	Verantwoordelijkheden en bevoegdheden
(Centrale-) onderne-mingsraad	De (Centrale) Ondernemingsraad heeft op basis van artikel 27, eerste lid, onder k en l van de Wet op de Ondernemingsraden instemmingsrecht ten aanzien van: 1. een regeling omtrent het verwerken van alsmede de bescherming van de persoonsgegevens van de in de onderneming werkzame personen; 2. een regeling inzake voorzieningen die gericht zijn op of geschikt zijn voor waarneming van of controle op aanwezigheid, gedrag of prestaties van de in de onderneming werkzame personen.

Functie	Verantwoordelijkheden en bevoegdheden
Auditor	Het team Concernaudit, onderdeel van de Staf Korpsleiding, heeft een onafhankelijke positie in de organisatie. Het periodiek auditen van de naleving van de bepalingen uit de Wpg is een wettelijke verplichting. Meer specifiek gaat het daarbij om:

[18] Taken en bevoegdheden Functionaris Gegevensbescherming, 6 maart 2019

Functie	Verantwoordelijkheden en bevoegdheden
	1. het uitvoeren van een jaarlijkse interne EDP-audit over een deel van de Wpg of over een deel van de organisatie op het gebied van de Wpg, zodanig dat in één cyclus van 4 jaar de gehele Wpg in de gehele organisatie is getoetst, ter voorbereiding op de externe privacyaudit; 2. het opstellen van een auditplan ter voorbereiding op de uitvoering van deze audit. Zorgdragen dat in het auditplan zijn opgenomen het doel, de inhoud, de doorlooptijd, de onderzoeksinstrumenten en de aanleverwijze en- termijn waarin de auditrapportage wordt opgeleverd; 3. zorgdragen voor de beveiliging en vertrouwelijkheid van de gegevens die door de audit worden gecontroleerd en de wijze waarop vastleggen in het auditplan. Hierbij ook aandacht hebben voor de geheimhoudingsplicht waar iedereen aan gebonden is; 4. opleveren van een auditrapportage met een beschrijving van de werkwijze en resultaten van de interne audit, alsmede het oordeel en de aanbevelingen van de auditor. Deze rapportage wordt aangeboden aan de korpschef; 5. uitvoeren van de hercontrole ter controle van de resultaten van het verbeterrapport dat namens de korpschef is opgesteld naar aanleiding van de eerdere externe audit. De resultaten van de hercontrole worden door de auditor in een rapportage opgesteld en aan de korpschef aangeboden.

7.3 Taken, rollen en verantwoordelijkheden privacy

Hiervoor zijn de verantwoordelijkheden en bevoegdheden die volgen uit de AVG, de Wpg, het mandaatbesluit en de governancestructuur benoemd. In deze paragraaf worden de taken, rollen en verantwoordelijkheden van de belangrijkste organisatieonderdelen en functionarissen ten aanzien van het beleid rond een rechtmatige en zorgvuldige verwerking van persoonsgegevens beschreven.

Functie	Taken, rollen en verantwoordelijkheden
Medewerker	Elke medewerker is verantwoordelijk voor een rechtmatige en zorgvuldige verwerking van persoonsgegevens bij de uitvoering van zijn werkzaamheden, daarbij maakt hij waar mogelijk gebruik van specifiek beleid, procedures, uitvoeringskaders en werkinstructies.

Functie	Taken, rollen en verantwoordelijkheden
Landelijk portefeuille-houder	Is verantwoordelijk voor beleidsvorming rond de portefeuille en voorbereiding van besluitvorming. Hij zorgt dat bij de beleidsvorming in opzet aantoonbaar wordt voldaan aan een rechtmatige en zorgvuldige verwerking van persoonsgegevens. Dit betekent meer specifiek dat de landelijk portefeuillehouder bij de ontwikkeling stuurt op: 1. het toepassen van privacy & security by design, het uitvoeren van GEB's en het gebruik van standaardinstellingen; 2. het vastleggen van verwerkingsactiviteiten in het verwerkingsregister; 3. het toepassen van principes rond kwaliteit van gegevens en minimale gegevensverwerking; 4. het toepassen van het informatiebeveiligingsbeleid, waaronder de procedures rond de meldplicht datalekken; 5. het invulling geven aan de informatieplicht aan betrokkene, waaronder actualisering van het privacystatement; 6. het toepassen van beleid en procedures met betrekking tot bewaar- en verwerkingstermijnen; 7. het toepassen van beleid met betrekking tot doorgifte of verstrekking van persoonsgegevens, waaronder het gebruik van modellen voor verwerkersovereenkomsten, convenanten en artikel 20-beslissingen; 8. het toepassen van het beleid met betrekking tot logging; 9. het toepassen van het beleid met betrekking tot autoriseren.

Functie	Taken, rollen en verantwoordelijkheden
Lijnmanager	Zoals eerder gesteld wordt bij de taakuitvoering onderscheid gemaakt tussen korpsniveau, eenheidsniveau (politiechefs), districts- en sectorniveau en teamniveau, en bij de bedrijfsvoering gaat het om korpsniveau, directieniveau (directeur PDC), dienstniveau en afdelingsniveau. Dit wordt in dit beleid 'lijnmanagement' genoemd. Het lijnmanagement is binnen het geheel aan kaders verantwoordelijk voor een aantoonbare rechtmatige en zorgvuldige verwerking van persoonsgegevens binnen zijn organisatieonderdeel en voor de opzet, bestaan en werking van de organisatie daarvan. Dit betekent meer specifiek dat de lijnmanager in de uitvoering stuurt op: 1. Het toepassen van privacy by design, het uitvoeren van GEB's en het gebruik van standaardinstellingen; 2. het vastleggen van verwerkingsactiviteiten in het verwerkingsregister; 3. het toepassen van principes rond kwaliteit van gegevens en minimale gegevensverwerking; 4. het toepassen van het informatiebeveiligingsbeleid, waaronder de procedures rond de meldplicht datalekken; 5. het invulling geven aan de informatieplicht aan betrokkene, waaronder actualisering van het privacystatement; 6. het toepassen van beleid en procedures met betrekking tot bewaartermijnen; 7. het toepassen van beleid met betrekking tot doorgifte of verstrekking van persoonsgegevens, waaronder het gebruik van modellen voor verwerkersovereenkomsten, convenanten en artikel 20-beslissingen; 8. het toepassen van het beleid met betrekking tot logging; 9. het toepassen van het beleid met betrekking tot autoriseren.

Functie	Taken, rollen en verantwoordelijkheden
Chief Information Officer	Is verantwoordelijk voor het uitdragen van IV aspecten in de organisatie, waaronder de rechtmatige en zorgvuldige verwerking van persoonsgegevens. Hij is tevens verantwoordelijk voor de organisatiebrede informatiebeveiliging.

Functie	Taken, rollen en verantwoordelijkheden
Gegevens-autoriteit	De Gegevensautoriteit ontwikkelt voor de politie het beleid voor een rechtmatige en zorgvuldige verwerking van persoonsgegevens en ondersteunt op die wijze de korpsleiding. Dit betekent meer specifiek dat de Gegevensautoriteit: 1. (Strategische) beleid, kaders en richtlijnen ontwikkelt op het gebied van een rechtmatige en zorgvuldige verwerking van persoonsgegevens; 2. totstandkoming van wet- en regelgeving met betrekking tot het verwerken van persoonsgegevens beïnvloedt; 3. de korpsleiding en de CIO adviseert over beleid, kaders en richtlijnen op het gebied van een rechtmatige en zorgvuldige verwerking van persoonsgegevens; 4. tweedelijns advisering en inzicht biedt aan privacyfunctionarissen in de eenheden en het PDC ten aanzien van het toepassen van geldende wet- en regelgeving en beleid bij gecompliceer-de vraagstukken en casuïstiek; 5. relevante ontwikkelingen en innovaties, binnen en buiten de politie, volgt en betrekt bij het gevoerde beleid dan wel initiatief neemt tot nieuw beleid; 6. informeel contact met de Autoriteit Persoonsgegevens onderhoudt.

Functie	Taken, rollen en verantwoordelijkheden
Concern Information	Is onderdeel van de IV, van de Staf Korpsleiding. De CISO ontwikkelt voor de politie het nformatiebeveiligingsbeleid. Dit betekent voor een rechtmatige en zorgvuldige verwerking van

Functie	Taken, rollen en verantwoordelijkheden
Security Officer (CISO)	persoonsgegevens meer specifiek dat de CISO beleid, kaders en richtlijnen ontwikkelt op het gebied van: 1. De meldplicht datalekken, waaronder het bijhouden van een register van incidenten; 2. autorisaties; 3. logging; 4. het laten uitvoeren van risicoanalyses in het kader van een GEB; 5. het formuleren van te nemen informatiebeveiligingsmaatregelen in het geval een gegevensverwerking wordt uitbesteed aan, dan wel in samenwerking met, een externe partij moet gaan plaatsvinden.

Functie	Taken, rollen en verantwoordelijkheden
Architectuur functie	Architectuur geeft aan hoe de organisatie, de informatievoorziening en andere ondersteunende diensten ingericht zouden moeten zijn om de organisatiedoelen te realiseren. De architectuur moet richting geven aan ontwerpkeuzes voor het benutten van de nieuwe informatiemogelijkheden en tevens een solide basis bieden voor betrouwbare werkprocessen en samenwerking met externe partners[19]. Dit betekent voor een rechtmatige en zorgvuldige verwerking van persoons-gegevens meer specifiek dat de architectuurfunctie de principes zoals beschreven in het *Uitvoeringskader privacy & security by design* als randvoorwaarde hanteert bij het richting geven aan ontwerpkeuzes. De architectuurfunctie draagt er bovendien aan bij dat dit uitvoeringskader doorontwikkeld wordt.

Functie	Taken, rollen en verantwoordelijkheden
Privacyfunc-tionaris (adviesrol)	Alleen binnen de Wpg hebben de privacyfunctionarissen een wettelijke taak, maar in beginsel hebben privacyfunctionarissen ten aanzien van de AVG dezelfde rol en bevoegdheden. In de eenheden is de privacyfunctionaris gepositioneerd bij het team bestuursondersteuning van de staf van de eenheid. Binnen het Politiedienstencentrum is de privacyfunctionaris gepositioneerd bij het privacyteam PDC van de staf. De privacyfunctionaris adviseert over de rechtmatige en zorgvuldige verwerking van persoonsgegevens, meer specifiek betekent dit dat hij adviseert over: 1. het toepassen van privacy by design, het uitvoeren van GEB's en het gebruik van standaardinstellingen; 2. het vastleggen van verwerkingsactiviteiten in het verwerkingsregister; 3. het toepassen van principes rond kwaliteit van gegevens en minimale gegevensverwerking; 4. het toepassen van het informatiebeveiligingsbeleid, waaronder de procedures rond de meldplicht datalekken; 5. het invulling geven aan de informatieplicht aan betrokkene, waaronder de afhandeling van verzoeken in het kader van rechten van betrokkene; 6. het toepassen van beleid en procedures met betrekking tot bewaartermijnen; 7. het toepassen van beleid met betrekking tot doorgifte of verstrekking van persoonsgegevens, waaronder het gebruik van modellen voor verwerkersovereenkomsten, convenanten en artikel 20-beslissingen; 8. het toepassen van het beleid met betrekking tot logging; 9. het toepassen van het beleid met betrekking tot autoriseren. Zo nodig raadpleegt hij een andere privacyfunctionaris in afzonderlijke gevallen. Ingeval van generieke toepassingsvraagstukken en van advisering aan de portefeuillehouder Wpg of AVG wordt een advies opgesteld in het verband van het Privacyplatform[20].

[19] Werken onder architectuur, Visie en inrichting van de architectuurfunctie, 25 januari 2018

[20] Privacyplatform bestaat uit alle privacyfunctionarissen van de eenheden, het PDC en de Politieacademie, alsmede vertegenwoordigers van de Gegevensautoriteit en het team Juridische zaken van de Staf Korpsleiding, met agendaleden van het Team Informatiebeveiliging, de KMar, de Rijksrecherche en de Bijzondere Opsporingsdiensten.

Functie	Taken, rollen en verantwoordelijkheden
	Daarnaast geeft de privacyfunctionaris voorlichting op het gebied van de naleving van de Wpg en AVG.

Functie	Taken, rollen en verantwoordelijkheden
Privacydesk	In elke eenheid wordt gewerkt aan de inrichting van een privacydesk, ondergebracht bij de staf, afdeling bestuursondersteuning. Met het inrichten van een privacydesk wordt expertise rond drie privacyprocessen samengebracht, wordt efficiency georganiseerd, kwaliteit geborgd, uniformiteit bevorderd en de werkvloer ontlast. Dit volgende processen zijn bij de privacydesks ondergebracht: 1. afhandeling verzoeken in het kader van rechten van de betrokkene; 2. convenantenbeheer; 3. afhandeling schriftelijke verzoeken tot (externe) verstrekking van persoonsgegevens.

Functie	Taken, rollen en verantwoordelijkheden
Competence Centre Wpg en AVG	Adviseert, binnen de taken en verantwoordelijkheden van de dienst IM van het PDC in het IV proces, hoe de Wpg en de AVG generiek en praktisch toepasbaar kunnen worden gemaakt. Daarnaast geeft het Competence Centre invulling aan de integrale aanpak van gegevensbescher-ming vanuit de dienst IM. Dit betekent meer specifiek dat het Competence Centre: 1. Voor de dienst ICT en de dienst IM advies geeft over privacy en security; 2. op verzoek privacy en security- templates ontwikkelt of daarover adviseert; 3. bijdraagt aan het creëren van awareness op het gebied van privacy en security binnen de organisatie; 4. een signaalfunctie heeft naar leidinggevenden waar het gaat om de vraag of ten aanzien van privacy en security 'de goede dingen worden gedaan' en eventueel daarbij helpt de juiste escalatielijnen te vinden en te gebruiken.

Functie	Taken, rollen en verantwoordelijkheden
Team Informatie-beveiliging	Het Team Informatiebeveiliging (TIB) van de sector gegevensgebruik en –beheer, is onderdeel van de dienst IM van het PDC. Daarnaast is sprake van een functionele aansturing door de CISO. Het TIB voert het informatiebeveiligingsbeleid uit. Dit betekent voor een rechtmatige en zorgvuldige verwerking van persoonsgegevens meer specifiek dat het TIB: 1. Risicoanalyses uitvoert op de beveiligingsaspecten over het onderwerp van een GEB; 2. adviseert over te nemen informatiebeveiligingsmaatregelen naar aanleiding van een uitgevoerde risicoanalyse; 3. aanspreekpunt is voor de meldplicht datalekken en meldingen van incidenten beoordeelt, afhandelt en registreert; 4. adviseert over beveiligingseisen die voldoen aan geldende wet- en regelgeving omtrent de bescherming van persoonsgegevens; 5. ondersteunt portefeuillehouders en lijnmanagers bij het autoriseren.

Functie	Taken, rollen en verantwoordelijkheden
Bevoegd functionaris (Wpg)	De bevoegd functionaris speelt een cruciale rol in het rechtmatig omgaan met persoonsgegevens bij alle vormen van gerichte gegevensverwerking (artikel 9 en 10-verwerkingen). Voor de verdere verwerking van politiegegevens, zogeheten doelafwijkend gebruik, is instemming vereist van een 'daartoe bevoegd functionaris'. Uit het model Aanwijzingsbesluit bevoegd functionaris volgt welke

Functie	Taken, rollen en verantwoordelijkheden
	functionarissen als zodanig worden aangewezen.[21] Er wordt een registratie bijgehouden van de bevoegd functionarissen die zijn aangewezen. Deze registratie is centraal raadpleegbaar. Voor een rechtmatige en zorgvuldige verwerking van persoonsgegevens betekent dit meer specifiek dat de bevoegd functionaris de volgende taken heeft: 1. het tijdig aanmelden van het doel van de verwerking; 2. het autoriseren van personen voor het verwerken van gegevens; 3. toetsen van voorgenomen doelafwijkend gebruik van persoonsgegevens aan de regels van de Wpg; 4. ter beschikking stellen van persoonsgegevens: instemmen, weigeren of beperken; 5. erop toezien dat binnen zijn onderzoek de herkomst en wijze van verkrijgen van de gegevens wordt geregistreerd; 6. afmelden van artikel 9-verwerkingen; schonen, ter bewaring aanbieden; 7. zorgen dat gegevens rechtmatig worden verwerkt.[22]

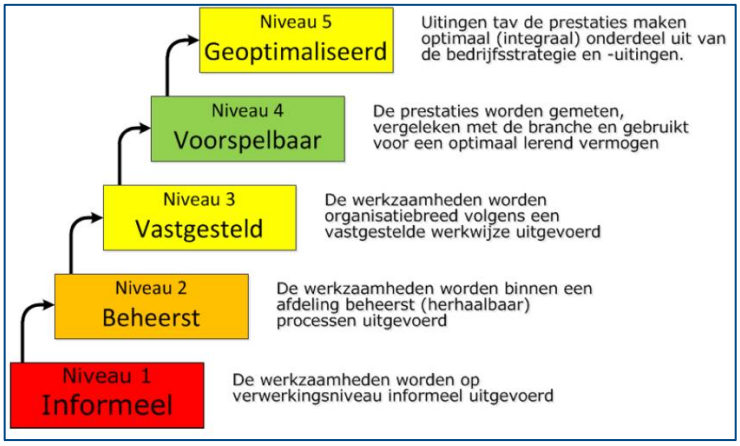
Functie	Taken, rollen en verantwoordelijkheden
Poortwachter (Wpg)	De poortwachter is een rol die aan een select aantal functionarissen binnen de Dienst Regionale Informatie Organisatie van de eenheden is toegekend. Deze poortwachters zorgen ervoor dat gegevens onder voorwaarden hernieuwd verwerkt kunnen worden en dat gegevens die onterecht geautomatiseerd zijn verwijderd alsnog via een zorgvuldig proces ontsloten kunnen worden.

Functie	Taken, rollen en verantwoordelijkheden
Control	Control faciliteert de organisatie en het verantwoordelijk management bij de beheersing van privacy en stelt de organisatie in staat op privacyaspecten aantoonbaar in control te komen. Daartoe faciliteert control: 1. bij het maken van afspraken over privacy met de omgeving (opgaven, beheerplan, begroting) en intern (beleid, korpsopdrachten, eenheidsopdrachten en eenheidsbijdrage aan korpsopdrachten); 2. dat getoetst wordt of de minimale privacy doelstellingen in de kaderbrief zijn bevestigd in de (meer)jaarplannen; en 3. over de voortgang van het bereiken van de minimale doelstellingen een beeld wordt gegeven in de managementrapportages. Daarmee is privacy onderdeel van de reguliere planning- & controlcyclus, met de bijbehorende verdeling van taken, verantwoordelijkheden en bevoegdheden en de bijbehorende systematiek voor de vaststelling van de kaderbrief en de (meer-)jaarplannen, periodieke rapportages en het voeren van managementgesprekken.

[21] Model Aanw jzingsbesluit bevoegd functionaris, vastgesteld door KMTO op 9 mei 2018
[22] Naslagwerk Bevoegd Functionaris, 5 september 2014

Bijlage 1 Privacy volwassenheidsmodel

Het privacybeleid sluit aan bij de niveaus het Privacy Volwassenheidsmodel van het Centrum voor Informatiebeveiliging en Privacybescherming[23] (CIP). Hieronder volgt een uitgebreide uitwerking per niveau.



Niveau 1- Informeel
Op niveau 1 verzamelt en verwerkt de politie gegevens, waarbij de keuzes per gegevens-verwerking op verwerkingsniveau worden gemaakt vanuit persoonlijk perspectief en afhankelijk zijn van de kennis en kunde van individuele medewerkers. Hierbij ontbreekt het aan formele processen om eisen te stellen aan de verwerking van persoonsgegevens en worden er informeel keuzes gemaakt over hoe er in een concreet geval wordt omgegaan met persoonsgegevens en op welke wijze de gegevens worden verzameld en (verder) verwerkt. Dit betekent dat op dit niveau wel vastlegging kan plaatvinden, maar dat er geen sprake is van vast*stelling*.
Er is geen managementcyclus, waardoor reactief wordt gereageerd op keuzes en incidenten die zich voordoen.

Niveau 2 – Beheerst proces
Op niveau 2 verzamelt en verwerkt de politie gegevens, waarbij keuzes worden gemaakt op basis van operationeel beleid, richtlijnen en werkinstructies dat door de verwerkingsverantwoordelijken wordt gedeeld en niet meer per gegevensverwerking wordt gepaald. Op dit niveau zijn het beleid, de richtlijnen en werkinstructies per afdeling vastgelegd, maar sluiten niet noodzakelijkerwijs aan op de politieorganisatiebrede omgang met gegevens. Daardoor is de werkwijze op afdelingsniveau wel traceerbaar, herhaalbaar en gestandaardiseerd, maar nog niet organisatiebreed. *De politieorganisatie leert slechts op lokaal afdelingsniveau*. De verschillende afdelingen kunnen wel van elkaar leren.
Er is wel structurele rapportage over bescherming van gegevens op projectniveau en afdelingsniveau, maar nog geen structurele rapportage van afdelingsniveau naar het hogere management.
Het kan zijn dat er op politieorganisatieniveau wel beleid is, maar dit wordt door de afdelingen niet altijd gehanteerd. Op politieorganisatieniveau kan wel privacybeleid zijn vastgelegd, maar niet officieel bekrachtigd en de controleprocessen om aan dit beleid te voldoen zijn niet organisatiebreed ingericht.

Niveau 3 – Vastgesteld proces
Op niveau 3 verwerkt de politie gegevens, waarbij keuzes zijn en worden gemaakt op basis van operationeel beleid, richtlijnen en werkinstructies op organisatieniveau. Het beleid is formeel vastgesteld op organisatieniveau en daarmee bekrachtigd als beleid voor de gehele politieorganisatie. De vereisten vanuit de organisatie zijn ook vertaald maar de inrichting van de context, de systemen en de beheerprocessen. *De politieorganisatie leert bedrijfsbreed*, omdat er een systematische samenhang bestaat tussen de uitvoerende onderdelen, beleidsonderdelen en controleonderdelen op alle niveaus. Er is structurele evaluatie van en rapportage over de rechtmatige gegevensverwerking (en beveiliging van

[23] Het CIP volwassendheidsmodel is beschikbaar op https://www.cip-overheid.nl/category/producten/gegevens-bescherming

gegevens) naar het hogere management, wat tot aanpassing van het organisatiebrede beleid kan leiden. Er bestaat sturing op de naleving van het beleid, richtlijnen en (werk)instructies. In tegenstelling tot niveau 2 wordt de sturing afgestemd met de bestuurder. De korpsleiding is betrokken bij de handhaving van het beleid en de uitvoering, waarbij gerapporteerd wordt ondersteund door controlemiddelen en informatie. Dit leidt tot een lerend proces op alle niveaus.

Niveau 4 – Voorspelbaar proces
Op niveau 4 verzamelt en verwerkt de politie gegevens, waarbij gestuurd wordt op snelheid en kwaliteit van de interacties. De operationele werkelijkheid wordt voortdurend bewaakt en aangepast om de organisatiebrede beleidsdoelen te behalen. Het lerend vermogen in de uitvoerende en specifiek beleidsmatige laag is op niveau 4 tot een maximum *voorspelbaar*.
Het management van de organisatie heeft op ieder gewenst moment inzicht in de stand van zaken omtrent de bescherming van gegevens in de gegevensverwerkingen en kan die vergelijken met die van de branche. Dit maakt transparantie naar buiten toe mogelijk en de prestatie van de organisatie zichtbaar en meetbaar.

Niveau 5 – Geoptimaliseerd
Op niveau 5 is er een sterk en expliciet (traceerbaar) verband tussen externe eisen, beveiligingsdoelstellingen, algemeen beleid, specifiek beleid en uitvoering. Aan alle keuzes ligt een uitgebreide, nauwkeurige analyse ten grondslag. Dit resulteert in de mogelijkheid om de politieorganisatie dynamisch aan te passen op basis van praktische ervaringen en prognoses van buiten de eigen organisatie. De operationele werkelijkheid en effectiviteit van beleid worden voortdurend bewaakt. Externe ontwikkelingen, zoals veranderende wet- en regelgeving of maatschappelijke factoren, kunnen snel en soepel worden vertaald naar nieuw specifiek beleid en uitvoering. Bovendien is de organisatie in staat om vooraf prognoses af te geven over kosten en reactiesnelheid. Daardoor zijn weloverwogen keuzes en trefzekere uitkomsten mogelijk. De bewaking en rapportage naar het hogere management is mede gebaseerd op de relatie tussen externe factoren en intern het algemeen beleid, specifiek beleid en de uitvoering. De prestatie-indicatoren zijn eenvoudig traceerbaar en vergelijkbaar met andere organisaties. Het lerend vermogen is op alle lagen tot een maximum geoptimaliseerd, door de verregaande geautomatiseerde feedbacklussen op alle lagen.

Bijlage 2 Privacybeleids- en uitvoeringskaders

1. Uitvoeringskader Privacy & Security by Design, versie 2.0, 23 april 2018
2. Beleidskader logging, versie 1.0, 1 mei 2018
3. Autorisatiebeleid, versie 1.0, 27 januari 2016
4. Informatiebeveiligingsbeleid, versie 1.1b, januari 2019
5. Beleidskader autoriseren externen voor politiegegevens
6. Werkinstructies Kompol
7. Handleiding rechten van betrokkene
8. Procesbeschrijving meldplicht datalekken
9. Verstrekkingenwijzer, december 2018
10. Handleiding informatieverstrekking op verzoek, 2019
11. Regeling periodieke audit politiegegevens