PUR MER END

GEMEENTEBLAD

Officiële uitgave van de gemeente Purmerend

Nr. 457423

31 oktober 2024

Beleidsregels Wet Politiegegevens gemeente Purmerend

Het college van burgemeester en wethouders van de gemeente Purmerend,

gelet op artikel 4a van de Wet politiegegevens,

B E S L U I T:

vast te stellen de navolgende Beleidsregels Wet Politiegegevens gemeente Purmerend

Artikel 1 Begripsbepalingen

In dit beleid wordt verstaan onder:

a) het college: het college van de burgemeester en wethouders van de gemeente Purmerend als verwerkingsverantwoordelijke van de politiegegevens;
b) buitengewoon opsporingsambtenaar: de buitengewoon opsporingsambtenaar die belast is met de opsporing van de strafbare feiten als bedoeld in artikel 142, tweede lid, van het Wetboek van Strafvordering;
c) Wpg: de Wet politiegegevens;
d) politiedomein: domein bestaande uit de politie, Koninklijke Marechaussee, Rijksrecherche, Bijzondere Opsporingsdiensten en de buitengewoon opsporingsambtenaren;
e) AVG: de Algemene verordening gegevensbescherming;
f) politiegegevens: elk persoonsgegeven dat wordt verwerkt in het kader van de uitvoering van de politietaak zoals bedoeld in artikel 1, aanhef en onder a, van de Wet politiegegevens;
g) verwerken van politiegegevens: elke bewerking of elk geheel van bewerkingen met betrekking tot politiegegevens of een geheel van politiegegevens, al dan niet uitgevoerd op geautomatiseerde wijze, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, samenbrengen, met elkaar in verband brengen, afschermen of vernietigen van politiegegevens;
h) verwerker: de natuurlijke persoon of rechtspersoon, overheidsinstantie, dienst of enig ander orgaan die of dat ten behoeve van de verwerkingsverantwoordelijke politiegegevens verwerkt. Indien een verwerker in strijd met het bij of krachtens deze wet bepaalde de doeleinden en middelen van de verwerking bepaalt, wordt die verwerker met betrekking tot die verwerking als verwerkingsverantwoordelijke aangemerkt;
i) register: het register van verwerkingen waarin de verwerkingen van politiegegevens, zoals bedoeld in artikel 31d van de Wet politiegegevens, zijn opgenomen.
j) Datalek: een inbreuk op de beveiliging van politiegegevens met de vernietiging, het verlies, de wijziging, de bekendmaking of de ter beschikkingstelling van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte politiegegevens tot gevolg;
k) DPIA: Data Protection Impact Assessment, een instrument om vooraf bij nieuwe of bestaande verwerkingen de risico's van een gegevensverwerking in kaart te brengen en op basis daarvan de maatregelen te nemen om de risico's te mitigeren;
l) bevoegd functionaris: een daartoe aangewezen functionaris, die over voldoende kennis en vaardigheden beschikt en bevoegd is om specifieke taken op grond van artikel 9 van de Wet politiegegevens uit te voeren.

Artikel 2 Inleiding

Het college heeft buitengewoon opsporingsambtenaren in dienst die belast zijn met zowel bestuursrechtelijke toezicht- als strafrechtelijke opsporingstaken op verschillende terreinen. Het betreft buitengewoon opsporingsambtenaren die actief zijn op het gebied van toezicht en handhaving van de openbare ruimte, het onderwijs en werk en inkomen.

De buitengewoon opsporingsambtenaren in de openbare ruimte zorgen voor de handhaving van de leefbaarheid binnen de gemeente Purmerend. De buitengewoon opsporingsambtenaren op het gebied van onderwijs richten zich op de handhaving van de Leerplichtwet 1969 en gerelateerde wet- en regelgeving. De buitengewoon opsporingsambtenaren op het gebied van werk en inkomen verrichten onderzoeken naar fraude met betrekking tot uitkeringen, met als doel fraude op het gebied van werk en inkomen te bestrijden.

In het kader van de bovengenoemde werkzaamheden verwerken de buitengewoon opsporingsambtenaren persoonsgegevens. Persoonsgegevens die in het kader van toezichtstaken worden verwerkt,

vallen onder de reikwijdte van de AVG. Persoonsgegevens die worden verwerkt in het kader van de opsporing van strafbare feiten, vallen onder de Wpg. Deze gegevens worden aangeduid als politiegegevens.

De Wpg stelt strikte eisen aan de manier waarop politiegegevens worden verzameld, verwerkt, bewaard en gedeeld. Om ervoor te zorgen dat deze verwerking van politiegegevens op een correcte en rechtmatige wijze plaatsvindt, is het noodzakelijk om heldere richtlijnen en beleidsregels te hanteren die voldoen aan de eisen van de Wpg. Daartoe is dit beleid vastgesteld, dat een gedetailleerd overzicht biedt van de beleidsregels die het college treft ten behoeve van de bescherming van politiegegevens.

Artikel 3 Het doel van dit beleid
Het doel van dit beleid is om een duidelijk en gedetailleerd kader te bieden voor de verwerking van politiegegevens door buitengewoon opsporingsambtenaren en andere ambtenaren, die niet direct belast zijn met opsporingstaken maar wel specifieke onderdelen van de opsporingstaken uitvoeren. Dit beleid is erop gericht om ervoor te zorgen dat de verwerking van politiegegevens op een rechtmatige, zorgvuldige en veilige wijze plaatsvindt.

Artikel 4 De reikwijdte van dit beleid
Dit beleid is van toepassing op alle verwerkingen van politiegegevens die worden uitgevoerd door buitengewoon opsporingsambtenaren en andere ambtenaren die geautoriseerd zijn om politiegegevens te verwerken.

Artikel 5 Het aanwijzen van de buitengewoon opsporingsambtenaar
De minister van Justitie en Veiligheid verleent aan buitengewoon opsporingsambtenaren, op verzoek van het college en indien aan de voorwaarden is voldaan, een akte van opsporingsbevoegdheid . Daarnaast worden buitengewoon opsporingsambtenaren beëdigd door de korpschef van de politie. De akte van opsporingsbevoegdheid specificeert de opsporingsbevoegdheden, die gelden in het grondgebied van de gemeente Purmerend.

Indien de buitengewoon opsporingsambtenaren buiten het grondgebied van Purmerend werkzaam zullen zijn, zal het college daartoe, na instemming van de (direct) toezichthouder en het driehoek, een samenwerkingsovereenkomst sluiten.

Artikel 6 Her- en bijscholing van de buitengewoon opsporingsambtenaar
De buitengewoon opsporingsambtenaren zijn gediplomeerd en bevoegd om hun uiteenlopende en complexe verantwoordelijkheden uit te voeren, die variëren van strafrechtelijke opsporingstaken tot bestuursrechtelijke toezichtstaken. Om hun kennis en vaardigheden actueel te houden, zijn de buitengewoon opsporingsambtenaren verplicht om voortdurend her- en bijscholing te volgen.

Het college voorziet in de benodigde her- en bijscholingsmogelijkheden, zodat de buitengewoon opsporingsambtenaren hun kennis kunnen actualiseren en verder verdiepen. Daarnaast biedt het college, ter ondersteuning van de buitengewoon opsporingsambtenaren, naast regelingen ook specifieke instructies aan die gericht zijn op het verwerken van politiegegevens. Deze instructies, zijn in overeenstemming met de Wpg en verschaffen gedetailleerde informatie voor een correcte verwerking van politiegegevens.

Verder organiseert het college jaarlijks bewustwordingsprogramma's voor de buitengewoon opsporingsambtenaren en andere medewerkers die in hun functie met politiegegevens in aanraking komen. Deze programma's zijn gericht op het verhogen van het bewustzijn en het up-to-date houden van de kennis.

Artikel 7 Het verlenen van de toegang tot politiegegevens
In overeenstemming met artikel 6 van de Wpg verleent het college toegang tot politiegegevens uitsluitend aan buitengewoon opsporingsambtenaren, indien deze toegang noodzakelijk is voor de uitvoering van hun specifiek toegewezen opsporingstaken. In uitzonderlijke gevallen verleent het college ook toegang tot politiegegevens aan andere ambtenaren, die niet direct belast zijn met opsporingstaken, maar waarvan hun taken indirect betrekking hebben op opsporingstaken.

Toegang tot politiegegevens is strikt gebonden aan een geheimhoudingsplicht. Voorafgaand aan de autorisatie worden daarom zowel de buitengewoon opsporingsambtenaren als andere betrokken medewerkers nadrukkelijk geïnformeerd over hun geheimhoudingsplicht en de juridische consequenties van schending van deze plicht.

Het college draagt in dit kader zorg voor dat de toegang tot politiegegevens periodiek wordt gecontroleerd. Deze controles omvatten onder meer het regelmatig controleren van de actualiteit van verleende autorisaties. Daarnaast draagt het college zorg voor het 'loggen' van de autorisaties conform artikel 32a van de Wpg, waarbij de gelogde gegevens uitsluitend worden ingezet voor de controle van de

rechtmatigheid van de verwerking van de politiegegevens. De bevindingen van de periodieke controles worden ter ondersteuning van de jaarlijks verplichte audits bewaard voor een periode van vijf jaar.

Artikel 8 Het verwerken van politiegegevens op grond van artikel 8 van de Wpg
Het college neemt passende maatregelen om ervoor te zorgen dat de verwerking van politiegegevens in overeenstemming is met de Wpg en de daarbij behorende regelingen en besluiten. Hierbij ziet het college erop toe dat politiegegevens uitsluitend worden verwerkt wanneer dit strikt noodzakelijk is voor het vervullen van opsporingstaken, zoals bepaald in artikel 3 van Wpg.

Daarnaast neemt het college conform artikel 4 van de Wpg, maatregelen om te waarborgen dat de politiegegevens te allen tijde juist en volledig zijn. Indien blijkt dat politiegegevens niet langer juist of volledig zijn, zorgt het college voor onmiddellijke correctie of vernietiging en voert zij periodieke controles uit om de juistheid van de politiegegevens te waarborgen.

Voorts zorgt het college ervoor dat buitengewoon opsporingsambtenaren, in overeenstemming met artikel 4, derde lid, van de Wpg, een duidelijk onderscheid maken tussen feitelijke informatie en persoonlijke oordelen. Eveneens waarborgt het college dat buitengewoon opsporingsambtenaren, conform de eisen gesteld in artikel 6b van de Wpg, een helder onderscheid maken tussen verschillende categorieën betrokkene(n), zoals verdachten, slachtoffers en derden.

Artikel 9 Het verwerken van politiegegevens op grond van artikel 9 van de Wpg
Naast de opsporingstaken zoals bedoeld in artikel 8 van de Wpg, verwerken buitengewoon opsporingsambtenaren in voorkomende gevallen politiegegevens indien dit noodzakelijk is voor een specifiek onderzoek naar een strafbaar feit, zoals bedoeld in artikel 9 van de Wpg.

In aanvulling op de waarborgen die het college treft, zoals genoemd in artikel 8 van dit beleid, draagt het college zorg dat voor deze specifieke verwerking een bevoegd functionaris wordt aangewezen. De verwerking op grond van artikel 9 van de Wpg vindt alleen plaats na instemming van de daartoe bevoegde functionaris. Deze functionaris is verantwoordelijk voor het waarborgen dat zowel de verwerking van politiegegevens als het doel van de verwerking binnen een week na aanvang van de verwerking correct worden vastgelegd. Daarnaast ziet de bevoegd functionaris erop toe dat de herkomst en wijze van verkrijging van de politiegegevens, evenals andere relevante informatie in het kader van het onderzoek, correct worden vastgelegd. De functionaris zorgt er ook voor dat de geldende bewaartermijnen strikt worden nageleefd.

Artikel 10 De termijnen van politiegegevens
Het verwerken van politiegegevens dient te voldoen aan de wettelijke bewaartermijnen. Het college treft in dat kader, conform artikel 14 van de Wpg, waarborgen om ervoor te zorgen dat politiegegevens niet langer worden bewaard dan strikt noodzakelijk is voor de uitvoering van de specifiek aan buitengewoon opsporingsambtenaren toegewezen opsporingstaken. Dit houdt in dat het college zorg draagt dat politiegegevens:

a. gedurende een jaar beschikbaar zijn in het kader van de uitvoering van de opsporingstaak;
b. na een jaar slechts beschikbaar zijn voor het gericht zoeken;
c. na vijf jaar worden verwijderd, maar worden niet vernietigd ten behoeve van klachtenafhandeling en audit doeleinden;
d. na tien jaar definitief worden vernietigd.

Voor verwerkingen in het kader van artikel 9 van de Wpg gelden afwijkende bewaartermijnen zoals in de Wpg bepaald. Het college treft in dit kader waarborgen om ervoor te zorgen dat politiegegevens niet langer worden bewaard dan noodzakelijk voor het doel van het onderzoek en dat de politiegegevens daarna tot maximaal een half jaar worden bewaard om te beoordelen of deze aanleiding geven tot een nieuw onderzoek of nieuwe verwerking, waarna deze voor een periode van vijf jaar slechts toegankelijk zullen zijn voor klachtenafdelingen en/of privacy audits. Na deze periode worden de politiegegevens definitief vernietigd.

Artikel 11 Het ter beschikking stellen en verstrekken van politiegegevens
In het kader van de uitvoering van de opsporingstaken die buitengewoon opsporingsambtenaren uitvoeren, kan het in voorkomende gevallen noodzakelijk zijn dat zij politiegegevens met anderen moeten delen. Het delen van politiegegevens kent twee vormen. Enerzijds betreft het hierbij het ter beschikking stellen van politiegegevens, en anderzijds het verstrekken van politiegegevens. Elke vorm van het delen van politiegegevens kent conform de Wpg een eigen regime en voorwaarden.

Bij het ter beschikking stellen van politiegegevens, in overeenstemming met artikel 15 van de Wpg, hanteert het college het principe van 'Free flow of information'. Dit principe faciliteert de uitwisseling van politiegegevens binnen het politiedomein, waardoor buitengewoon opsporingsambtenaren in

voorkomende gevallen de politiegegevens met de politie of andere relevante partijen binnen het politiedomein, ter beschikking kunnen stellen indien dit noodzakelijk is voor de uitoefening van hun taken.

Bij de verstrekking van politiegegevens aan externe partijen buiten het politiedomein, zoals bepaald in paragraaf 3 van de Wpg, draagt het college zorg voor dat de verstrekking voldoet aan de wettelijk gestelde voorwaarden. Hierbij wordt het 'need to know'-principe gehanteerd, wat zorgt dat uitsluitend politiegegevens worden verstrekt, overeenkomstig de wettelijke vereisten en enkel met wettelijk bepaalde instanties. Het college draagt zorg voor dat elke vorm van verstrekking van politiegegevens door de buitengewoon opsporingsambtenaar, conform artikel 32, eerste lid, aanhef en onder b, van de Wpg, zorgvuldig wordt gedocumenteerd.

Bij de verstrekking van politiegegevens aan externe partijen buiten het politiedomein draagt het college bovendien zorg voor dat de ontvangende partij wordt geïnformeerd over de geheimhoudingsplicht die op hen rust. De ontvangende partij wordt tevens voorzien van de noodzakelijke informatie waarmee de juistheid, volledigheid en actualiteit van de ontvangen gegevens kunnen worden beoordeeld. Indien er sprake is van onjuistheden in de politiegegevens, wordt de ontvangende partij de mogelijkheid geboden om contact op te nemen om de onjuistheden in de gegevens te corrigeren.

Het college draagt tenslotte zorg voor dat politiegegevens niet ter beschikking worden gesteld of worden verstrekt aan ontvangers in derde landen, tenzij voldaan is aan de gestelde voorwaarden zoals genoemd in artikel 17a van de Wpg.

Artikel 12 De beveiliging en bescherming van politiegegevens

Het college neemt passende beheersmaatregelen om te waarborgen dat de procesinrichting voor de verwerking van politiegegevens, zowel in ontwerp als in uitvoering, overeenstemt met de Baseline Informatiebeveiliging Overheid. Deze baseline is het algemene normenkader voor de technische en organisatorische maatregelen binnen de overheid. Het college voldoet aan deze normen en neemt passende technische en organisatorische maatregelen om een beveiligingsniveau te garanderen dat is afgestemd op de risico's die verbonden zijn aan de verwerking van (bijzondere categorieën van) politiegegevens. In dit kader hanteert het college de principes van 'privacy by design', 'privacy by default', 'security by design' en 'security by default' bij de verwerking van politiegegevens. Dit houdt in dat bij de ontwikkeling en het ontwerp van applicaties en systemen, evenals bij het inrichten van verwerkingsprocessen, gegevensbeschermings- en informatiebeveiligingsmaatregelen worden geïntegreerd.

Het college voert, in overeenstemming met artikel 4c van de Wpg, daarnaast een beoordeling uit op de impact van de gegevensbescherming op verwerkingen die potentieel een hoog risico vormen voor de rechten en vrijheden van personen, het zogenaamde DPIA. Deze beoordeling is gericht op het identificeren en mitigeren van deze risico's door effectieve beveiligingsmaatregelen te implementeren

Artikel 13 Samenwerking met verwerkers

Het college maakt voor de verwerking van politiegegevens mogelijk gebruik van applicaties, oftewel IT-systemen, die beheerd en onderhouden worden door serviceorganisaties. De serviceorganisatie wordt aangemerkt als verwerker. De selectie van de verwerkers geschiedt met de hoogste mate van zorgvuldigheid, waarbij enkel verwerkers in aanmerking komen die aantoonbaar voldoen aan de vereiste technische en organisatorische maatregelen. Het college legt de samenwerking met de verwerkers, in lijn met artikel 6c, tweede lid, van de Wpg, vast in een schriftelijke overeenkomst, inclusief de bijbehorende verwerkersovereenkomst, waarbij het actuele model van de standaardovereenkomst van de Vereniging Nederlandse Gemeenten wordt gebruikt.

Het college vereist daarbij dat de verwerkers de benodigde informatie verstrekken om aan verplichtingen, zoals genoemd in de artikelen 6, 32, 32a en 33 van de Wpg, te kunnen nakomen.

Artikel 14 De rechten van de betrokkene(n)

Het college hecht grote waarde aan het nauwkeurig informeren van de betrokkene(n) over de wijze waarop politiegegevens worden verwerkt. Op de website van de gemeente Purmerend wordt een algemene uitleg gegeven over de wijze waarop het college persoons- en politiegegevens verwerkt. Daarnaast wordt inzicht geboden in de rechten van de betrokkene(n) en de procedurele stappen die zij kunnen nemen om deze rechten uit te oefenen.
Daarnaast stelt het college betrokkene(n) in staat om, naast de rechten van betrokkenen op grond van de AVG, ook rechten met betrekking tot de verwerking van hun politiegegevens uit te oefenen conform paragraaf 4 van de Wpg. Hiervoor heeft het college een procedure ontwikkeld die zowel betrekking heeft op de AVG als op de Wpg. Deze procedure beschrijft op welke wijze verzoeken worden afgehandeld, wie daarbij welke verantwoordelijkheid heeft, en hoe het college de betrokkene(n) van informatie voorziet.

In deze procedure is tevens informatie opgenomen onder welke omstandigheden het college niet kan voldoen aan een specifiek verzoek, met name wanneer het verstrekken van informatie het onderzoek naar of de vervolging van een strafbaar feit zou kunnen belemmeren. De gronden voor het afwijzen van een verzoek zijn omschreven in artikel 27, tweede lid, van de Wpg.

In voorkomende gevallen, indien er sprake is van uitzonderingsgronden zoals vastgelegd in artikel 27, tweede lid, van de Wpg, kan het college niet aan een verzoek tegemoetkomen. Deze weigeringsgronden zien op situaties waarin het verstrekken van informatie een ernstige belemmering zou vormen voor de opsporing of vervolging van strafbare feiten of bijvoorbeeld als de informatieverstrekking de rechten en vrijheden van anderen zou schaden. In dergelijke gevallen waarborgt het college dat de belangen van de betrokkene zorgvuldig worden afgewogen in het licht van de in de wet vastgelegde uitzonderingsgronden. Indien het college besluit een verzoek af te wijzen, zal dit besluit schriftelijk worden gemotiveerd en de betrokkene(n) worden geïnformeerd over de toepasselijke weigeringsgrond.

Artikel 15 Het behandelen van datalekken

Het college erkent dat, ondanks haar inspanningen om datalekken te voorkomen, er in de complexe wereld van gegevensbeheer en -beveiliging toch situaties kunnen ontstaan waarin een datalek zich voordoet.

Op de website van de gemeente Purmerend wordt informatie verstrekt over wat een datalek inhoudt en hoe betrokkene(n) een datalek bij de gemeente Purmerend kunnen melden. Hierin wordt onder andere uitgelegd aan inwoners en anderen, indien nodig, dat zij een datalek tevens kunnen melden bij de Autoriteit Persoonsgegevens.

Wanneer een datalek plaatsvindt, handelt het college direct om de risico's voor de betrokkene(n) te minimaliseren. Hiervoor is een procedure voor datalekken opgesteld, die tevens betrekking heeft op datalekken op grond van artikel 33a van de Wpg. In deze procedure is beschreven op welke wijze datalekken worden afgehandeld, wie welke verantwoordelijkheid draagt, en hoe het college voorziet in corrigerende maatregelen om de risico's ten gevolge van het datalek te mitigeren.

In het geval dat een datalek zich voordoet waarbij een midden of hoog risico bestaat voor de rechten en vrijheden van betrokkene(n), meldt het college dit onverwijld bij de Autoriteit Persoonsgegevens en, indien noodzakelijk, aan de betrokkene(n) zelf. Op grond van artikel 33a, zevende lid, van de Wpg kan de mededeling aan de betrokkene echter worden uitgesteld, beperkt of achterwege worden gelaten, wanneer de gronden zoals vermeld in artikel 27, tweede lid, van toepassing zijn.

Het college onderhoudt daarnaast een zorgvuldig bijgehouden register van datalekken die zowel op grond van de AVG als op grond van de Wpg plaatsvinden. Dit register dient niet alleen als een instrument voor verantwoording en transparantie naar de betrokkene(n) en toezichthouders, maar dient tevens als bron voor het analyseren van de oorzaken van datalekken. Op basis van deze analyses implementeert het college gerichte verbeteringen om de kans op herhaling van datalekken te verminderen.

Artikel 16 Het register van verwerkingen

Het college beschikt over een register van verwerkingen, waarin ook de verwerkingen van politiegegevens op grond van artikel 31d van de Wpg zijn opgenomen. Dit register bevat onder andere de volgende informatie:

- De gegevens van het college, optredend als verantwoordelijke voor de verwerking van de politiegegevens.
- De specifieke doeleinden waarvoor politiegegevens worden verwerkt, om duidelijkheid te verschaffen over de redenen voor het verzamelen en gebruiken van deze informatie.
- Een beschrijving van de categorieën persoonsgegevens die worden verwerkt, om inzicht te bieden in de aard van de verwerkte informatie.
- Een overzicht van de categorieën betrokkene(n), om te verduidelijken van wie politiegegevens worden verwerkt.
- Een lijst van de categorieën ontvangers aan wie politiegegevens ter beschikking kunnen worden gesteld of verstrekt, om een duidelijk beeld te geven van de wijze waarop en met wie informatie wordt gedeeld.

Daarnaast zorgt het college ervoor dat het register voortdurend wordt geactualiseerd en jaarlijks wordt getoetst. Deze actualisatie waarborgt dat alle informatie in het register actueel en correct is, en stelt het college daarmee in staat om de Wpg-verwerkingsactiviteiten voortdurend te evalueren en waar nodig, te verbeteren.

Artikel 17 Het uitvoeren van een privacy-audit

Het college voert in overeenstemming met artikel 33 van de Wpg controles uit in de vorm van privacy-audits op processen waarin politiegegevens worden verwerkt.

De privacy-audits vinden jaarlijks plaats in de vorm van interne audits. Daarnaast wordt er iedere vier jaar een externe audit uitgevoerd waarvoor het college een meerjarig auditplan ontwikkelt, dat de reikwijdte, planning en methodiek van de audits omvat. Mocht uit de resultaten van de privacy-audits blijken dat bepaalde onderdelen in het proces niet voldoen aan de Wpg, dan neemt de het college verbetermaatregelen om deze tekortkomingen te adresseren en te verhelpen.

Artikel 18 De Functionaris Gegevensbescherming
Naast het zorgvuldig uitvoeren van audits zoals beschreven in dit beleid, heeft het college een Functionaris Gegevensbescherming aangewezen, een onafhankelijke toezichthouder wiens kerntaak het is om conform de Wpg, toezicht te houden op het verwerken van politiegegevens.

De verantwoordelijkheden van de Functionaris Gegevensbescherming zijn uitgebreid en divers. Conform artikel 36 van de Wpg vervult de Functionaris Gegevensbescherming enkele adviserende taken en houdt daarnaast toezicht op het voldoen aan de wettelijke normen met betrekking tot de verwerking van politiegegevens door het college. De toezichtstaken omvatten, maar zijn niet beperkt tot, toezicht op:

- de bewustwording over en naleving van de verplichtingen omtrent het verwerken van politiegegevens;
- het autorisatieproces voor toegang tot politiegegevens;
- de kwaliteit en nauwkeurigheid van de politiegegevens;
- de naleving van de vastgestelde bewaartermijnen;
- de correcte verstrekking van politiegegevens;

Daarbij stelt de Functionaris Gegevensbescherming jaarlijks rapportages op, inclusief aanbevelingen voor verbeteringen of wijzigingen in de processen.

Artikel 19 De herziening en evaluatie van dit beleid
Dit beleid wordt ten minste elke drie jaar geëvalueerd en, indien nodig, herzien om de actualiteit, effectiviteit en naleving ervan te waarborgen.

Artikel 20 Slotbepaling
Dit besluit treedt in werking op de dag na die van bekendmaking.

Aldus vastgesteld in de vergadering d.d. 15 oktober 2024.

Purmerend,

burgemeester en wethouders van Purmerend,

de wnd. secretaris,
M.H. van der Weit

de burgemeester,
E. van Selm