GEMEENTE VLISSINGEN

GEMEENTEBLAD

Officiële uitgave van de gemeente Vlissingen

Nr. 320053

6 juli

2026

WPG beleid gemeente Vlissingen 2026

Het college van burgemeester en wethouders van de gemeente Vlissingen;
gelet op artikel 4a van de Wet politiegegevens en de artikelen 4:81, 4:83 en 1:3, vierde lid, van de Algemene wet bestuursrecht;
overwegende dat het wenselijk is beleidsregels vast te stellen over de naleving en uitvoering van de Wet politiegegevens binnen de gemeentelijke boa-organisatie;

besluit vast te stellen:

Wpg-beleid gemeente Vlissingen 2026.

Inleiding

Dit beleid heeft tot doel vast te leggen hoe de gemeente Vlissingen voldoet aan de verplichtingen uit de Wet politiegegevens bij de verwerking van politiegegevens door of namens de gemeentelijke boa's. Dit beleid is van toepassing op alle medewerkers, boa's, leidinggevenden, beheerders en andere geautoriseerde functionarissen die betrokken zijn bij het verwerken, beheren, raadplegen, verstrekken, beveiligen of vernietigen van politiegegevens binnen de gemeente Vlissingen.
Het beleid heeft in ieder geval betrekking op Domein I: Openbare Ruimte.

Afbakening AVG/Wpg

De AVG is van toepassing op persoonsgegevens die worden verwerkt in het kader van toezichtstaken of andere niet-opsporingsgerichte gemeentelijke taken. De Wpg is van toepassing zodra persoonsgegevens worden verwerkt in het kader van de opsporingstaak van de boa. Wanneer gegevens die aanvankelijk in het kader van toezicht zijn verzameld vervolgens worden gebruikt voor de opsporingstaak, worden deze gegevens aangemerkt als politiegegevens en is de Wpg van toepassing.

Artikel 1 Begripsbepaling

In dit beleid wordt verstaan onder:
a. gemeente Vlissingen: het college van burgemeester en wethouders als verwerkingsverantwoordelijke van de politiegegevens;
b. buitengewoon opsporingsambtenaar: de buitengewoon opsporingsambtenaar als bedoeld in het Besluit buitengewoon opsporingsambtenaar;
c. opsporingstaak: de opsporing van de strafbare feiten als bedoeld in artikel 142, tweede lid, van het Wetboek van Strafvordering;
d. akte van opsporingsbevoegdheid: de akte van opsporingsbevoegdheid als bedoeld in artikel 142, eerste lid, onder a, van het Wetboek van Strafvordering;
e. wet: de Wet politiegegevens, het Besluit politiegegevens, het Besluit politiegegevens voor buitengewoon opsporingsambtenaar en de Regeling periodieke audit politiegegevens;
f. beschikbaar studiemateriaal: het Praktijkhandboek van de Wet politiegegevens, de Verstrekkingenwijzer en het Naslagwerk Verstrekken op grond van de Wet politiegegevens;
g. Wpg-domein: domein bestaande uit de politie, marechaussee, rijksrecherche, Bijzondere Opsporingsdiensten en de buitengewoon opsporingsambtenaren;
h. politiegegevens: persoonsgegevens die in het kader van de uitoefening van de politietaak worden verwerkt;
i. verwerken van politiegegevens: elke handeling of elk geheel van handelingen met betrekking tot politiegegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, vergelijken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van politiegegevens;
j. autorisatiebeleid: het autorisatiebeleid voor het toewijzen, wijzigen en intrekken van autorisaties ten behoeve van de toegang tot politiegegevens;
k. verwerker van politiegegevens: degene die, niet werkzaam binnen de gemeentelijke organisatie, het geheel of een gedeelte van het geautomatiseerde systeem onder zich heeft waarmee de politiegegevens worden verwerkt.

Artikel 2 Algemeen beleid

1. De organisatie hanteert het volgende beleid, tenzij door de directie een tijdelijke afwijking daarvan wordt besloten.

2. De organisatie hanteert als raamwerk voor beheersmaatregelen het door Wpg-auditoren gehanteerde control framework, zoals dat is opgenomen in bijlage 3 en 4 van de NOREA-handreiking privacy audit Wpg voor boa's.
3. Wanneer gebruik wordt gemaakt van een informatiesysteem dat wordt beheerd door een leverancier, bijvoorbeeld CityControl, wordt met de leverancier een verwerkersovereenkomst afgesloten en dient deze jaarlijks een Third Party Memorandum conform de NOREA-handreiking privacy audit Wpg voor boa's te overleggen.
4. De organisatie voert voor elke verwerking van politiegegevens een DPIA uit. Deze DPIA wordt elke drie jaar herzien. Deze is verplicht omdat het gaat om gevoelige gegevens en sprake is van een ongelijke machtsverhouding tussen de boa en de verdachte. Daarin worden de volgende principes getoetst en geborgd:

a. gegevensbescherming door beveiliging en ontwerp;
b. gegevensbescherming door standaardinstellingen.

5. Voor zover het de applicatie betreft, worden de in het vierde lid genoemde principes tevens afgedekt in de TPM.
6. De organisatie verwerkt politiegegevens op basis van artikel 8 van de Wpg, voor zover dit noodzakelijk is voor de uitvoering van de dagelijkse politietaak.
7. De organisatie stelt politiegegevens ter beschikking of verstrekt politiegegevens uitsluitend voor zover daarvoor een grondslag bestaat in de Wpg, waaronder de artikelen 15 tot en met 21 Wpg. Rechtstreekse verstrekkingen op grond van artikel 23, 23a en 24 Wpg vinden niet plaats, tenzij daarvoor een afzonderlijke wettelijke grondslag bestaat en hierover vooraf advies is ingewonnen bij de Functionaris Gegevensbescherming.
8. De organisatie verwerkt geen gegevens op basis van:

a. artikel 9 Wpg, onderzoek in een bepaald geval. Wel verlenen boa's medewerking aan onderzoeken onder verantwoordelijkheid van de politie of andere opsporingsdiensten;
b. artikel 11 Wpg, geautomatiseerd vergelijken en in combinatie zoeken voor een artikel 9-onderzoek;
c. artikel 13 Wpg, ondersteunende taken, voor zover die gegevens onder verantwoordelijkheid van instanties worden verwerkt;
d. artikel 15a Wpg, terbeschikkingstelling binnen de Europese Unie;
e. artikel 17 Wpg, verstrekkingen aan inlichtingen- en veiligheidsdiensten;
f. artikel 17a Wpg, doorgifte aan derde landen, dat wil zeggen landen buiten de Europese Economische Ruimte;
g. geautomatiseerde besluitvorming, waaronder profilering als bedoeld in artikel 7a Wpg.

9. Toegangsbeveiliging is zodanig ingericht dat alleen boa's en geautoriseerden toegang hebben tot politiegegevens.
10. Bij de verzending van politiegegevens worden deze altijd versleuteld verstuurd.
11. Er zijn geen gemeenschappelijke verwerkingen van politiegegevens.
12. De logging mag uitsluitend worden gebruikt ter controle van de rechtmatigheid en ter waarborging van de integriteit en de beveiliging van politiegegevens en voor strafrechtelijke procedures.

Artikel 3 Rollen, taken en bevoegdheden

1. De Privacy Officer is verantwoordelijk voor het beheer van het verwerkingenregister en de privacyverklaring op de website.
2. De Privacy Officer inventariseert jaarlijks of het bereik van de verwerkingen met politiegegevens is gewijzigd. Op basis daarvan worden dit beleid en het verwerkingenregister indien nodig door de Privacy Officer aangepast.
3. De coördinator van de boa's heeft de volgende taken:

a. jaarlijks inventariseren of de leveranciers nog steeds beschikken over een actuele TPM en/of ISO 27001-certificering;
b. het onder de aandacht brengen van de handreiking en gedragsregels voor boa's bij de medewerkers en het toezien op deze gedragsregels;
c. het bijhouden van een overzicht met geautoriseerden;
d. zorgen dat artikel 8-gegevens:
i. na één jaar alleen nog beschikbaar zijn voor gericht zoeken;
ii. na vijf jaar worden verwijderd, dat wil zeggen alleen beschikbaar zijn voor audits en klachtenprocedures;
iii. na tien jaar worden vernietigd;
e. het ieder kwartaal controleren op logging en toegangsrechten om ervoor te zorgen dat alleen de daarvoor bevoegde personen gegevens kunnen inzien en er geen misbruik gemaakt kan worden van deze bevoegdheid;
f. het ieder kwartaal controleren van de kwaliteit van processen-verbaal en de naleving van de daarvoor geldende werkinstructies;

g. het vastleggen van de bevindingen uit de kwartaalcontroles en het, indien nodig, bespreken daarvan met de teamleider VTH.
4. De CISO is verantwoordelijk voor het laten uitvoeren van Wpg-audits.
5. De teamleider VTH is verantwoordelijk voor de implementatie en uitvoering van de Wpg en heeft in dat kader onder andere de volgende taken:

a. actueel houden van het verwerkingenregister ten aanzien van verwerkingen in het team;
b. bijhouden van een lijst met veel voorkomende verstrekkingen met daarbij de onderbouwing van de grondslag voor de verstrekking;
c. het laten uitvoeren van DPIA's;
d. het bewaken dat bevindingen uit controles, audits of kwaliteitsbeoordelingen waar nodig worden opgevolgd met passende organisatorische of technische maatregelen.
6. De teamleider VTH heeft de volgende bevoegdheden:

a. het nemen van autorisatiebesluiten in de zin van artikel 6, derde, vierde en vijfde lid, Wpg, met behulp van het formulier "Autorisatie verwerking politiegegevens";
b. het besluiten over toegang tot informatiesystemen met politiegegevens, waaronder het vaststellen van de autorisatiematrix voor het informatiesysteem waarin politiegegevens worden verwerkt;
c. het vaststellen van werkinstructies, procesbeschrijvingen en gerelateerde documenten.
7. De applicatiebeheerder bewaakt de beveiliging van de applicatie, onder andere door logbestanden te analyseren.
8. De Functionaris Gegevensbescherming:

a. adviseert en informeert over de Wpg, onder andere over DPIA's;
b. houdt toezicht op de uitvoering van de Wpg op basis van een toezichtsplan;
c. werkt samen met de Autoriteit Persoonsgegevens en is contactpunt voor de Autoriteit Persoonsgegevens;
d. stelt jaarlijks een verslag op met bevindingen.
9. Interne audits en externe Wpg-audits worden gecoördineerd door de CISO conform Nota AD 1336715.
10. Betrokkenen worden geïnformeerd over de verwerking van politiegegevens via de website en, indien van toepassing, bij de eerste brief die zij ontvangen over strafrechtelijke handhaving.

Artikel 4 Specifiek beleid ten aanzien van team VTH, Domein I: Openbare ruimte
1. De organisatie gebruikt naast bestuursrechtelijke middelen ook strafrechtelijke instrumenten voor toezicht en handhaving in de openbare ruimte.
2. Daarom zijn binnen dit taakveld boa's aangesteld en is de Wpg van toepassing.

Artikel 5 Specifiek beleid ten aanzien van Domein II: Milieu, welzijn en infrastructuur
1. De organisatie heeft de taken met betrekking tot handhaving op het gebied van de Omgevingswet belegd bij de Omgevingsdienst RUD Zeeland en bij toezichthouders milieu van de gemeente.
2. De toezichthouders milieu van de gemeente voeren deze taken alleen bestuursrechtelijk uit.
3. Daarom zijn binnen dit taakveld geen boa's aangesteld bij de gemeente.

Artikel 6 Specifiek beleid ten aanzien van politiegegevens bij de uitvoering van de Leerplichtwet, Domein III: Onderwijs
1. Deze taak is neergelegd bij de gemeente Middelburg.
2. Daarom zijn binnen dit taakveld geen boa's aangesteld bij de gemeente.

Artikel 7 Specifiek beleid ten aanzien van politiegegevens bij de uitvoering van de Participatiewet, Domein V: Werk, inkomen en zorg
1. Deze taak is neergelegd bij GR Orionis.
2. Daarom zijn binnen dit taakveld geen boa's aangesteld bij de gemeente.

GEMEENTE VLISSINGEN

Artikel 8 Rechten van betrokkenen

1. Betrokkenen worden geïnformeerd over de verwerking van politiegegevens via de privacyverklaring op de website van de gemeente Vlissingen en, indien van toepassing, bij de eerste brief die zij ontvangen over strafrechtelijke handhaving.
2. Verzoeken van betrokkenen op grond van de Wpg, waaronder verzoeken om informatie, inzage, rectificatie, vernietiging of beperking van de verwerking, worden behandeld volgens de daarvoor geldende interne procedure.
3. Bij de beoordeling van verzoeken van betrokkenen wordt rekening gehouden met de uitzonderingsgronden uit de Wpg, waaronder het belang van opsporing, vervolging en handhaving.

Artikel 9 Datalekken

1. Een vermoedelijke inbreuk op de beveiliging van politiegegevens wordt onverwijld gemeld volgens de interne procedure voor datalekken.
2. Datalekken met betrekking tot politiegegevens worden geregistreerd in het datalekregister.
3. Indien de Wpg daartoe verplicht, wordt de inbreuk gemeld bij de Autoriteit Persoonsgegevens en, indien nodig, aan betrokkenen.
4. Bij de beoordeling en afhandeling van datalekken wordt rekening gehouden met de aard van de politiegegevens, de mogelijke gevolgen voor betrokkenen en het belang van opsporing en handhaving.

Artikel 10 Werkinstructies en geheimhouding

1. De gemeente Vlissingen voorziet in werkinstructies en gedragsregels voor de verwerking van politiegegevens door boa's en andere geautoriseerde functionarissen.
2. Boa's en andere geautoriseerde functionarissen nemen deze werkinstructies en gedragsregels in acht bij de verwerking van politiegegevens.
3. Boa's en andere geautoriseerde functionarissen verwerken geen politiegegevens indien deze niet noodzakelijk zijn voor de uitvoering van de aan hen opgedragen taak.
4. Boa's en andere geautoriseerde functionarissen zijn verplicht tot geheimhouding van politiegegevens, tenzij een wettelijk voorschrift tot verstrekking verplicht of uit hun taak de noodzaak tot verstrekking voortvloeit.
5. In de werkinstructies wordt een specifieke procedure opgenomen voor de aanstelling, functiewijziging en uitdiensttreding van boa's en andere geautoriseerde functionarissen. Deze procedure borgt dat toegangsrechten en autorisaties tijdig worden toegekend, aangepast of ingetrokken en dat politiegegevens op juiste wijze worden bewaard, overgedragen, afgeschermd of vernietigd.
6. Bij overtreding van dit beleid, de werkinstructies of de geheimhoudingsplicht wordt gehandeld volgens het geldende HR-beleid.

Artikel 11 Audits en verbetermaatregelen

1. De gemeente Vlissingen toetst periodiek of de verwerking van politiegegevens voldoet aan de Wpg en de daarop gebaseerde regelgeving.
2. Jaarlijks wordt een interne Wpg-audit uitgevoerd.
3. Eenmaal per vier jaar wordt een externe Wpg-audit uitgevoerd door een onafhankelijke auditor.
4. Indien uit een interne of externe audit blijkt dat de verwerking van politiegegevens niet voldoet aan de geldende normen, worden verbetermaatregelen vastgesteld en uitgevoerd.
5. De opvolging van verbetermaatregelen wordt bewaakt door de CISO, in afstemming met de Functionaris Gegevensbescherming en de teamleider VTH.

Artikel 12 Register van verwerkingen

1. De gemeente Vlissingen houdt een register bij van verwerkingen van politiegegevens.
2. In het register wordt per verwerking in ieder geval opgenomen:

a. het doel van de verwerking;
b. de categorieën politiegegevens;
c. de categorieën betrokkenen;
d. de categorieën ontvangers;
e. de grondslag voor de verwerking of verstrekking;
f. de bewaartermijnen;
g. de getroffen technische en organisatorische beveiligingsmaatregelen.

3. Het register wordt actueel gehouden en jaarlijks beoordeeld op volledigheid en juistheid.

Artikel 13 Inwerkingtreding en citeertitel

1. Dit beleid treedt in werking op de dag na bekendmaking.
2. Dit beleid wordt aangehaald als: Wpg-beleid gemeente Vlissingen 2026.
3. Het eerdere Wpg-beleid van de gemeente Vlissingen wordt ingetrokken op het moment van inwerkingtreding van dit beleid.

Vlissingen, 16 juni 2026,
Burgemeester van Vlissingen,
de secretaris,
drs. R.D.A. Wiskerke
de burgemeester,
drs. A.R.B. van den Tillaar