Privacybeleid Wet politiegevens Gemeente Nissewaard

Tussen [rechte haken] staan verwijzingen naar het control framework van NOREA voor Wpg audits.

Vastgesteld door het college van burgemeester en wethouders op 4 juni 2024.

Algemeen beleid

1. De organisatie hanteert het volgende beleid, tenzij door de Directie een (tijdelijke) afwijking daarvan wordt besloten:

    a. De organisatie hanteert als raamwerk voor beheersmaatregelen (Control Framework) het door Wpg-auditoren gehanteerde raamwerk, zoals dat is opgenomen in bijlage 3 en 4 van de NOREA handreiking privacy audit Wpg voor boa's.
    b. Wanneer gebruik gemaakt wordt van een informatiesysteem dat wordt beheerd door een leverancier (bijvoorbeeld SaaS), dan wordt met de leverancier een verwerkersovereenkomst afgesloten en dient deze jaarlijks een Third Party Memorandum (TPM) conform de NOREA handreiking privacy audit Wpg voor boa's te overleggen. De teamleider controleert dit jaarlijks.
    c. De organisatie voert voor elke verwerking van politiegegevens een DPIA uit en deze wordt elke 3 jaar herzien.[8] (Deze is verplicht omdat het gaat om gevoelige gegevens en er sprake is van een ongelijk machtsverhouding tussen de Boa en de verdachte). Daarin worden de volgende principes getoetst en geborgd:
        i. Gegevensbescherming door beveiliging en ontwerp [6]
        ii. Gegevensbescherming door standaard-instellingen [7]

        Voor zover het de applicatie betreft worden deze principes tevens afgedekt in de TPM.
    d. De organisatie verwerkt politiegegevens op basis van
        i. Artikel 8 van de Wpg (uitvoering van de dagelijkse politietaak) en
        ii. op basis van de artikelen over ter beschikking stellen en verstrekking van politiegegevens (Art 15-21 en 23-24).
    e. De organisatie verwerkt *geen* gegevens op basis van
        i. Art 9 Wpg (onderzoek in een bepaald geval). Wel verlenen Boa's medewerking aan onderzoeken onder verantwoordelijkheid van de politie of andere opsporingsdiensten.
        ii. Art 11 Wpg (geautomatiseerd vergelijken en in combinatie zoeken voor een Art 9 onder-zoek) [18]
        iii. in het kader van Art 13 Wpg (ondersteunende taken), voor zover die gegevens onder verantwoordelijkheid van instanties worden verwerkt. [1, 13]
        iv. Art 15 Wpg voor zover het gaat om terbeschikkingstellingen binnen de EU

v. Art 17 Wpg (verstrekkingen aan inlichtingen en veiligheidsdiensten)
vi. Art 17a Wpg (Doorgifte aan derde landen, d.w.z. landen buiten de Europese Economische Ruimte) [22]
vii. Art 23, 23a en 24 Wpg (Rechtstreekse verstrekkingen)
viii. en maakt geen gebruik van geautomatiseerde besluitvorming, waaronder profilering als bedoeld in de Wpg Art 7a. [1, 17]

f. Toegangsbeveiliging is zodanig ingericht dat alleen Boa's en geautoriseerden toegang hebben tot politiegegevens.
g. Bij de verzending van politiegegevens worden deze altijd versleuteld verstuurd.

Rollen, taken en bevoegdheden

2. De Privacy Officer Wpg inventariseert jaarlijks:
    a. of het bereik van de verwerkingen met politiegegevens is gewijzigd. Op basis daarvan worden dit beleid en het verwerkingenregister indien nodig aangepast.
    b. of de leveranciers nog steeds beschikken over een actuele TPM en/of ISO27001 certificering.
    c. Is verantwoordelijk voor het op peil houden van de bewustwording bij de medewerkers binnen de gemeentelijke organisatie die werken met politiegegevens.

3. De CISO:
    a. Is toezichthouder informatiebeveiliging en houdt in die rol toezicht op de informatieveiligheidsaspecten voor het verwerken van politiegegevens, voornamelijk op basis van de Baseline Informatiebeveiliging Overheid.
    b. Moet actief worden betrokken bij de activiteiten inzake de TPM en/of ISO27001 certificering zoals genoemd onder de taken van de PO-Wpg en ondersteunt bij de beoordeling daarvan op het gebied van informatiebeveiliging.

4. De Teamleiders van de teams waar politiegegevens worden verwerkt zijn verantwoordelijk voor de implementatie en uitvoering van de Wpg en hebben in dat kader onder andere de volgende taken:
    a. Het informeren van de medewerkers over de handreiking/gedragsregels voor Boa's en het toezien op naleving van deze gedragsregels
    b. Het bijhouden van een overzicht met geautoriseerden
    c. Actueel houden van het verwerkingenregister t.a.v. verwerkingen in het team [26], in samenspraak met de PO-Wpg
    d. Bijhouden van een lijst met veel voorkomende verstrekkingen met daarbij de onderbouwing van de grondslag voor de verstrekking [20, 23]
    e. Het (laten) uitvoeren van DPIA's
    f. Zorgen dat Art 8 gegevens [16, 20]
        i. Na 1 jaar alleen nog beschikbaar zijn voor gericht zoeken
        ii. Na 5 jaar worden verwijderd, dat wil zeggen alleen beschikbaar zijn voor audits en klachtenprocedures
        iii. Na 10 jaar worden vernietigd.

5. De Teamleider van het team met daarin Boa's heeft de volgende bevoegdheden:
    a. Het nemen van autorisatiebesluiten in de zin van Wpg Art 6 lid 3, 4, 5 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.

De eenheidsmanager heeft dezelfde bevoegdheden voor het autoriseren van teamleiders.

6. De adviseur Toezicht bewaakt beveiliging van de applicatie, onder andere door autorisaties te controleren en log-bestanden te analyseren.

7. De Functionaris Gegevensbescherming Wpg
    a. adviseert en informeert over de Wpg, onder andere over DPIA's
    b. houdt toezicht op de uitvoering van de Wpg
    c. werkt samen met de AP en is contactpunt voor de AP
    d. stelt jaarlijks een verslag op met bevindingen
8. De FG Wpg voert de volgende controles uit en kan daarbij gebruik maken van de inzet van de PO-Wpg:
    a. Steekproefsgewijze beoordeling van Processen Verbaal, ten minste jaarlijks, op de volgende criteria:
        i. **Werken conform de gedragsregels [2]**
        ii. **Adequaat hanteren van doelbinding,**
        iii. **Noodzakelijkheid, rechtmatigheid, juiste en volledige verwerking van politiegegevens [3,4]**
        iv. **Vastlegging van de herkomst en wijze van verkrijging [4]**
        v. Alleen verwerken van bijzondere politiegegevens wanneer dit onvermijdelijk is [9]
        vi. Onderscheiding tussen feitelijke en subjectieve gegevens, c.q. feiten en persoonlijke oordelen [5]
        vii. Onderscheiden tussen verschillende categorieën van betrokkenen, zoals verdachten, slachtoffers, getuigen en veroordeelden. [12]
        viii. Vastlegging en rechtmatigheid van ter beschikkingstellingen en verstrekkingen [17, 21, 23, 24]
    b. Toetsen van tijdige uitvoering en/of actualisering van DPIA [8]
    c. Toetsen van het testen en evalueren van de doeltreffendheid van de beheersmaatregelen, waaronder beveiligingsmaatregelen bijvoorbeeld n.a.v. de DPIA [6, 31]
    d. Controle van Toewijzing van autorisaties en de controle daarvan door de systeemeigenaar [10]
    e. Controle van de verwerkersovereenkomst op actualiteit en actuele bijbehorende certificaten en verklaringen [13, 22, B4]
    f. Controle van bewustmaking en opleiding van Boa's en andere geautoriseerden [14]
    g. Controle van (nieuwe) arbeidsovereenkomsten, screening etc. [14]
    h. Controle van de hantering van afschermings-, verwijderings- en vernietigingstermijnen [16, 20]
    i. Controle van de rechtmatigheid van verstrekkingen [21,
    j. Controle van correcte en tijdige uitvoering en documentatie, o.a. van de reden van afwijzing van verzoeken van betrokkenen, zoals vernietiging en rectificatie van politiegegevens. [4, 25]

k. Toetsen van een adequate analyse van de logging [28]
l. Controle van correcte en tijdige opvolging van datalekken, zoals documentatie, analyse en meldingen aan AP en betrokkenen [30]
m. Controle van uitvoering van de audits en opvolging van de bevindingen[31]
n. Controle van volledigheid en juistheid van het verwerkingenregister voor zover het Wpg verwerkingen betreft.[3, 26]

9. Interne en externe Wpg audits worden gecoördineerd en/of uitgevoerd door het team Audit van de Eenheid Control & Informatie.
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.

Specifiek beleid ten aanzien van het Team VTH (Domein I: Openbare ruimte)

De organisatie gebruikt naast bestuursrechtelijke middelen ook strafrechtelijke instrumenten voor toezicht en handhaving in de openbare ruimte. Daarom zijn binnen dit taakveld Boa's aangesteld en is de Wpg van toepassing.

Specifiek beleid ten aanzien van het Team VTH (Domein II: Milieu, welzijn en infrastructuur)

De organisatie gebruikt naast bestuursrechtelijke middelen ook strafrechtelijke instrumenten voor toezicht en handhaving. Daarom zijn binnen dit taakveld Boa's aangesteld en is de Wpg van toepassing.

Specifiek beleid ten aanzien politiegegevens bij de uitvoering van de leerplichtwet (Domein III: Onderwijs)

De organisatie gebruikt naast bestuursrechtelijke middelen ook strafrechtelijke instrumenten voor toezicht en handhaving van de leerplichtwet, in het bijzonder Art 16 lid 5 en Art 26. Daarom zijn binnen dit taakveld Boa's aangesteld en is de Wpg van toepassing.

Specifiek beleid ten aanzien politiegegevens bij de uitvoering van de participatiewet (Domein V: Werk, Inkomen en Zorg)

De organisatie gebruikt alleen bestuursrechtelijke middelen voor toezicht en handhaving in het kader van de Participatiewet door de Sociale Recherche en Zorgwetgeving. Daarom zijn binnen dit taakveld geen Boa's aangesteld en is de Wpg niet van toepassing.