gemeente Overbetuwe

GEMEENTEBLAD

Officiële uitgave van de gemeente Overbetuwe

Nr. 478929

10 november 2023

Privacybeleid Wpg gemeente Overbetuwe 2023

Burgemeester en wethouders van de gemeente Overbetuwe;

gelet op artikel 4:81 e.v. van de Algemene wet bestuursrecht;

gelet op artikel(en) 24, tweede lid van de Algemene verordening gegevensbescherming en artikel 4a van de Wet politiegegevens;

b e s l u i t e n:

vast te stellen de

Privacybeleid Wpg gemeente Overbetuwe 2023

Artikel 1 Begripsomschrijvingen

Deze beleidsregel verstaat onder:

a. betrokkene: degene van wie persoonsgegevens wordt verwerkt ter uitvoering van een politietaak;
b. boa: buitengewoon opsporingsambtenaar, zijnde een beëidigd functionaris belast met opsporing van bepaalde strafbare feiten;
c. DPIA: Data Protection Impact Assessment, een onderzoek om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen;
d. NOREA: beroepsorganisatie van IT-auditors in Nederland;
e. politiegegeven: politiegegeven als bedoeld in artikel 1 van de Wet politiegegevens;
f. Wpg: Wet Politiegegevens;
g. [nr.]: verwijzing naar het control framework van NOREA voor Wpg audits.

Artikel 2 Toepassingsbereik

Dit beleid is van toepassing op de verwerking van politiegegevens.

Artikel 3 Algemeen

De gemeente hanteert het volgende beleid, tenzij door gemeentesecretaris een (tijdelijke) afwijking daarvan wordt besloten:

1. 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.
2. Wanneer gebruik gemaakt wordt van een informatiesysteem dat wordt beheerd door een leverancier (bijvoorbeeld SaaS[1]), dan wordt met de leverancier een verwerkersovereenkomst afgesloten en dient deze een Third Party Memorandum[2] (TPM) conform de NOREA handreiking privacy audit Wpg voor boa's te overleggen.
3. De organisatie voert voor elke verwerking van politiegegevens een DPIA uit en deze wordt elke 3 jaar herzien.[8]. Daarin worden de volgende principes getoetst en geborgd:
   a. gegevensbescherming door beveiliging en ontwerp [6];
   b. gegevensbescherming door standaard-instellingen [7].
4. De organisatie verwerkt politiegegevens op basis van artikel 8 van de Wpg (uitvoering van de dagelijkse politietaak) en op basis van de artikelen over ter beschikking stellen en verstrekking van politiegegevens (artikelen 15 tot en met 21, 23 en 24 Wpg).
5. 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) [18];

1) Saas: Software as a Service, stelt gebruikers in staat om via internet verbinding te maken met toepassingen in de cloud en deze te gebruiken. Voorbeelden zijn e-mail, agendafuncties en kantoorsoftware (zoals Microsoft Office 365).
2) Third Party Memorandum: een verklaring die afgegeven wordt door een onafhankelijk audit partij over de kwaliteit van een ICT-dienstverlening en – beheersing van een organisatie.

c. in het kader van artikel 13 Wpg (ondersteunende taken), voor zover die gegevens onder verantwoordelijkheid van instanties worden verwerkt, bijvoorbeeld door gegevens te leveren en/of te onttrekken aan het landelijk register bijtincidenten [1, 13];
d. artikel 17a Wpg (Doorgifte aan derde landen, d.w.z. landen buiten de Europese Economische Ruimte) [22].

6. De organisatie maakt geen gebruik van geautomatiseerde besluitvorming, waaronder profilering als bedoeld artikel 7a van de Wpg [1, 17]
7. Toegangsbeveiliging is zodanig ingericht dat alleen Boa's en geautoriseerden toegang hebben tot politiegegevens.
8. Bij de verzending van politiegegevens worden deze altijd versleuteld verstuurd.

Artikel 5 Rollen, taken en bevoegdheden

1. 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 aangepast.
2. De teammanager van het team met daarin Boa's is verantwoordelijk voor de implementatie en uitvoering van de Wpg en heeft in dat kader onder andere de volgende taken:
   a. Het onder de aandacht brengen van de handreiking/gedragsregels voor Boa's bij de medewerkers en het toezien op deze gedragsregels
   b. Het bijhouden van een overzicht met geautoriseerden
   c. Actueel houden van het verwerkingenregister ten aanzien van verwerkingen in het team [26]
   d. Bijhouden van een lijst met veel voorkomende verstrekkingen met daarbij de onderbouwing van de grondslag voor de verstrekking [20, 23]
   e. Zorgen dat artikel 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.

3. De teammanager van het team met daarin Boa's heeft de volgende bevoegdheden:
   a. Het nemen van autorisatiebesluiten in de zin van artikel 6, derde tot en met vijfde lid van de 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.

4. De applicatiebeheerder bewaakt beveiliging van de applicatie, onder andere door log-bestanden te analyseren.
5. De Functionaris gegevensbescherming:
   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 Autoriteit Persoonsgegevens en is contactpunt voor de Autoriteit Persoonsgegevens;
   d. stelt jaarlijks een verslag op met bevindingen.

6. De Functionaris gegevensbescherming (of Privacyofficer) voert de volgende controles uit:
   a. Steekproefsgewijze beoordeling van Processen Verbaal, ten minste jaarlijks, op de volgende criteria:
      i. **Werken conform de gedragsregels [2];**
      ii. **Adequaat hanteren van doelbinding oftewel of gegevens worden verwerkt en verzameld voor een welbepaald, uitdrukkelijk omschreven en gerechtvaardigde doel [2];**
      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 teammanager [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 een verzoek van betrokkene, 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].

7. Interne en externe Wpg audits worden gecoördineerd door de concerncontroller van de gemeente.
8. 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 t.a.v. Domein I (Openbare ruimte)
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.

Artikel 5 Specifiek beleid t.a.v. Domein II (Milieu, welzijn en infrastructuur)
De organisatie gebruikt alleen bestuursrechtelijke middelen voor toezicht en handhaving. Daarom zijn binnen dit taakveld geen Boa's aangesteld en is de Wpg niet van toepassing.

Artikel 6 Specifiek beleid t.a.v. Domein III (Onderwijs)
De organisatie gebruikt alleen bestuursrechtelijke middelen voor toezicht en handhaving. Daarom zijn binnen dit taakveld geen Boa's aangesteld en is de Wpg niet van toepassing.

Artikel 7 Specifiek beleid t.a.v. Domein V (Werk, Inkomen en Zorg)
De organisatie gebruikt alleen bestuursrechtelijke middelen voor toezicht en handhaving. Daarom zijn binnen dit taakveld geen Boa's aangesteld en is de Wpg niet van toepassing.

Artikel 8 Specifiek beleid t.a.v. politiegegevens bij de uitvoering van bouw- en woningtoezicht
De organisatie gebruikt alleen bestuursrechtelijke middelen voor toezicht en handhaving. Daarom zijn binnen dit taakveld geen Boa's aangesteld en is de Wpg niet van toepassing.

Artikel 9 Inwerkingtreding
De beleidsregel treedt in werking de dag na bekendmaking.

Artikel 10 Citeertitel
Deze beleidsregel wordt aangehaald als: Privacybeleid Wpg gemeente Overbetuwe 2023.

Aldus besloten op 24 oktober 2023.

Burgemeester en wethouders,

de gemeentesecretaris
P.J.E. Breukers

de burgemeester,
R.P. Hoytink-Roubos

Toelichting

Algemeen
Uit artikel 24 Algemene Verordening Gegevensbescherming en de Wet politiegegevens volgt dat de gemeente privacybeleid heeft ten aanzien van de verwerking van politiegegevens. Dit zijn gegevens die de boa's gebruiken voor de uitvoering van hun strafrechtelijke opsporingstaak. Het gaat dus niet om gegevens die de boa's gebruiken voor een bestuurlijke toezichtstaak.

De zwart gedrukte tekst in het beleid ziet op activiteiten die de FG (of PO) minimaal moet uitvoeren op grond van de Wpg.

Artikel 1 Begripsomschrijvingen
e. politiegegeven: het gaat om persoonsgegevens die boa's verwerken in het kader van hun opsporingstaak. Het gaat dus niet om gegevens die de boa's gebruiken voor een bestuurlijke toezichtstaak.

Artikel 3 Algemeen
Lid 3
De organisatie voert voor elke verwerking van politiegegevens een DPIA uit en deze wordt elke 3 jaar herzien. Deze is verplicht omdat het gaat om gevoelige gegevens en er sprake is van een ongelijk machtsverhouding tussen de Boa en de verdachte.

Artikel 5 Rollen, taken en bevoegdheden.
Lid 3 onder a
Bij het autoriseren van personen gaat het om andere medewerkers dan Boa's, bijvoorbeeld medewerkers die post met politiegegevens registreren of de functioneel beheerder van het systeem.