BMC

YACHT GROUP

Privacyscan Burgernet

Toetsing aan kaders Algemene Verordening Gegevensbescherming en Wet Politiegegevens

Rapport
Burgernet

BMC
November 2019
Classificatie: Vertrouwelijk
Status: Definitief

BMC Advies B.V.
P.O. box 490
3800 AL Amersfoort

Databankweg 26 D
3821 AL Amersfoort

T +31 (0)33 496 52 00
www.bmc.nl

KVK 32078667
IBAN NL91ABNA0504035754
BTW NL80.86.63.598 B.01

Inhoud

Hoofdstuk 1 Inleiding

1.1 Inleiding en werkwijze

De stuurgroep Burgernet heeft BMC gevraagd een privacyscan uit te voeren op de verwerkingen van persoonsgegevens in het kader van de uitvoering van taken door Burgernet.

Bij de uitvoeren van de privacyscan is aandacht besteed aan de volgende onderwerpen:

- vaststellen van het toepasselijk privacykader (Wpg of AVG);
- beoordeling van de vraag wie verwerkingsverantwoordelijke is en wie (sub)verwerkers;
- privacyaspecten verbonden aan de aanmelding waaronder grondslag, en noodzaak verwerking persoonsgegevens en verwijderingstermijnen;
- de inrichting van de autorisaties;
- de beschrijving van de procedures en werkinstructies;
- het afsluiten van verwerkersovereenkomsten;
- aspecten van informatiebeveiliging;
- transparantie naar betrokkenen;
- het herkennen en melden van datalekken;
- het behandelen van klachten en de uitoefening van rechten door betrokkenen;
- de uitwerking van informatie met betrekking tot beveiligingsvoorschriften (geen technische controle van systemen).

Deze privacyscan is uitgevoerd in de periode september tot december 2019. Hiervoor zijn gesprekken gevoerd met medewerkers van het LPB. Daarnaast zijn er documenten opgevraagd, in beeld gebracht en bestudeerd. Een overzicht van de gebruikte documenten en de geïnterviewde personen is opgenomen in bijlage 1 en 2. Een technische beoordeling van de werking van applicaties en databases behoort niet tot de opdracht. Dit betekent dat de beoordeling in deze privacyscan alleen gebaseerd is op documenten en verklaringen en dat er geen toetsing heeft plaatsgevonden van de feitelijke werking. Op 14 januari 2020 is de privacyscan besproken met de landelijke programmamanager Burgernet. De uitkomsten van deze bespreking zijn in deze privacyscan verwerkt.

1.2 Samenvatting

Deze privacyscan is uitgevoerd voor de verwerking van persoonsgegevens in het kader van de uitvoering van taken door Burgernet. Op basis van deze privacyscan zijn een aantal conclusies gegeven en aanbevelingen gedaan. Voor een overzicht hiervan wordt verwezen naar hoofdstuk 5 van deze rapportage. Samenvattend kan worden geconcludeerd dat bij de opzet van Burgernet zeer bewust aandacht is gegeven aan de privacyaspecten verbonden aan het programma. Daarbij is uitgegaan van een minimale gegevensverwerking, transparantie naar de deelnemers en de mogelijkheid om zelf de eigen gegevens te beheren, inclusief verwijdering daarvan.

Op een aantal onderdelen is echter nog verbetering mogelijk. Deze verbeteringen hebben met name betrekking op de formele afspraken en positionering van Burgernet. Niet in alle gevallen zijn formele rollen en verantwoordelijkheden in de samenwerking tussen de deelnemende partijen voldoende beschreven. Dat leidt in een aantal gevallen tot onduidelijkheid over formele verantwoordelijkheden. Uit de interviews is niet gebleken dat dit in de praktijk tot problemen heeft geleid. Om mogelijke onduidelijkheden in de toekomst te voorkomen, worden een aantal aanbevelingen gedaan. Deze hebben met name betrekking op het formaliseren van de rol van de Politie als verwerkingsverantwoordelijke, de rol van het LPB en de rol van de deelnemende gemeenten. Daarnaast worden enkele aanbevelingen gedaan om de transparantie naar betrokkenen te vergroten en de beveiligingseisen naar de verwerkers verder te specificeren.

1.3 Leeswijzer

Hoofdstuk 2 beschrijft het wettelijk kader dat gebruikt is bij de beoordeling in deze rapportage. Daarna komen het toetsingskader en de uitgevoerde werkzaamheden aan de orde in hoofdstuk 3. De bevindingen hebben een plaats gekregen in hoofdstuk 4. Het rapport sluit af met conclusies en aanbevelingen in hoofdstuk 5.

Hoofdstuk 2 Het wettelijk kader

2.1 De AVG en sectorale wetgeving

Deze privacyscan brengt de mogelijke privacyrisico's[1] in kaart bij deelname aan Burgernet. Daarbij is onder andere het proces van aan- en afmelden van deelnemers in beeld gebracht, evenals de werkwijze bij het doen uitgaan en intrekken van een Burgernetmelding. Op basis van de uitkomsten van deze privacyscan kunnen waar nodig gericht maatregelen worden ondernomen om eventuele risico's te verminderen. Daarnaast kan een privacyscan:

- de gevolgen van toezicht en handhaving verminderen;
- de kwaliteit van gegevens verbeteren;
- de dienstverlening verbeteren;
- de besluitvorming verbeteren;
- het privacybewustzijn binnen een organisatie verhogen;
- de haalbaarheid van een project verbeteren;
- het vertrouwen van de klanten, werknemers of burgers verstevigen in de wijze waarop persoonsgegevens worden verwerkt en privacy wordt gerespecteerd;
- de communicatie verbeteren over privacy en de bescherming van persoonsgegevens.

Tijdens de privacyscan is de gegevensverwerking beoordeeld tegen de achtergrond van de risico's van de verwerking voor de privacy van betrokkenen. De belangrijkste toetsingscriteria zijn:

- Rechtmatige grondslag: voor het verwerken van persoonsgegevens geeft de AVG een aantal grondslagen, waaronder de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag (artikel 6 lid 1 AVG). De Wet politiegegevens (Wpg) kent in artikel 8 een grondslag.
- Doelbinding: persoonsgegevens mogen alleen worden verwerkt voor een voorafgaand bekendgemaakt doel en alleen die gegevens mogen worden verwerkt die noodzakelijk zijn om het doel te bereiken (artikel 5 lid 1 onder b AVG en artikel 3 Wpg)).
- Transparantie: een betrokkene moet worden geïnformeerd over de verwerking van zijn persoonsgegevens (artikel 12 AVG en artikel 24 Wpg).
- Aspecten van beveiliging, waaronder autorisatie en controle op logging (artikel 5 lid 1 onder f en artikel 4a en 6 Wpg).
- Proportionaliteit: niet meer gegevens verwerken dan noodzakelijk is voor een bepaald doel (artikel 5 lid 1 onder c AVG en artikel 4 Wpg).
- Subsidiariteit: is het doel ook te bereiken met minder op de privacy ingrijpende middelen (artikel 5 lid 1 onder c AVG)?
- Bewaartermijnen: gegevens mogen niet langer worden bewaard in een vorm die het mogelijk maakt de betrokkene te identificeren dan noodzakelijk is voor de verwezenlijking van het doel waarvoor ze zijn verzameld (artikel 5 lid 1 onder e AVG en artikel 4 Wpg).

[1] Daarbij wordt opgemerkt dat deze privacyscan niet kwalificeert als een Data Protection Impact Assessment als bedoeld in artikel 35 lid 1 van de Algemene Verordening Gegevensbescherming (AVG).

Naast de AVG en Wpg is ook sectorale wetgeving van belang. In het kader van deze rapportage betreft dat de volgende wet- en regelgeving:

- de Gemeentewet;
- de Politiewet;
- regeling Informatiebeveiliging Politie.

Hoofdstuk 3 Feitelijke situatie

3.1 Organisatie van Burgernet

Burgernet is een samenwerking tussen gemeenten, Politie en burgers om samen te werken aan de veiligheid. Burgernetdeelnemers die zich via de website van Burgernet hebben aangemeld ontvangen een spraak- of sms-bericht wanneer er iets gebeurt in hun omgeving. Deelnemers die de Burgernetapp hebben gedownload krijgen een appbericht. Als de deelnemer een relevante waarneming heeft gedaan, dan kan deze via een telefoonnummer van de Politie worden gemeld (dit kan ook via de app met de telefoon). Er zijn 1,7 miljoen personen via de website van Burgernet aangemeld als deelnemer van Burgernet. De Burgernetapp is circa 800.000 – 900.000 keer gedownload. Er zijn circa 200.000 actieve gebruikers per maand. Het aantal is afhankelijk van het aantal alerts[2].

Het LPB werkt in opdracht van een stuurgroep Burgernet bestaande uit vertegenwoordigers van de Politie, de Vereniging Nederlandse Gemeenten (VNG), gemeenten en het Ministerie van Justitie en Veiligheid. Daarnaast is een Raad van Toezicht benoemd. Voor het LPB of de stuurgroep is geen publiek-privaatrechtelijke regeling of organisatievorm in het leven geroepen. Het LPB heeft geen formele positie of eigenstandige beslissingsbevoegdheid over de verwerking van persoonsgegevens in het kader van Burgernet. Wel kan het LPB in opdracht van de verwerkingsverantwoordelijke beheer- en ontwikkelingstaken op zich nemen.

Werkwijze Burgernet

Deelnemers kunnen zich via de website van Burgernet aanmelden[3]. Naast het aanmelden via de website kan ook gekozen worden voor het gebruik van de Burgernetapp of social media. Na aanmelding via een van de drie kanalen ontvangt de betrokkene van Burgernet meldingen. Deze meldingen hebben meestal betrekking op een persoon of een voertuig. Vaak gaat het om een vermissing, diefstal, een overval of een verdachte situatie. Of in een situatie gebruikgemaakt wordt van Burgernet is ter beoordeling aan de betreffende centralist van de meldkamer van de Politie. Hiervoor wordt een protocol gebruikt. Er worden in het Burgernetbericht geen identificerende kenmerken meegestuurd. Dit betekent dat een situatie, voertuig of locatie in algemene zin kan worden beschreven maar dat geen kentekens, namen, adresgegevens of andere identificerende gegevens in het Burgernetbericht worden opgenomen. Dat betekent niet dat daarmee een betrokkene nooit zou kunnen worden geïdentificeerd. Bij vermissingen, en met name bij (jonge) kinderen, is het zeer wel denkbaar dat buurtgenoten of andere betrokkenen de in het Burgernetbericht bedoelde persoon kunnen identificeren.

In enkele gevallen wordt in een dergelijke situatie door de persoon die via Burgernet is gezocht en gevonden op een later moment een verzoek tot verwijdering gedaan.

---

[2] Bij benadering stand per september 2019

[3] https://www.burgernet.nl/about#

Met name in situaties waarin een persoon op jongere leeftijd vermist is geweest. In dat geval wordt het bericht verwijderd en een beroep gedaan op Google. Een Burgernetbericht is altijd kortdurend (< 1 uur) en er wordt altijd een afloopbericht verstuurd; ook indien er geen persoon of voertuig is aangetroffen.

3.2 Functionele beschrijving Burgernet

3.2.1 Inleiding

De samenwerking tussen de Politie en de gemeenten heeft als doel samen te werken aan veiligheid. Dat doen partijen ieder vanuit een eigen verantwoordelijkheid. Bij de Politie is deze taak gelegen in het uitvoeren van de dagelijkse politietaak. Voor gemeenten geldt dat zij zich meer richten op preventie in het kader van het veiligheidsbeleid van een gemeente. De Politie en deelnemende gemeenten hebben voor het bereiken van deze doelen verschillende kanalen tot hun beschikking om de deelnemende burgers te bereiken:

- Burgernetapp
- Twitter
- Facebook Messenger
- Sms-berichten via telefoon aan deelnemers
- Spraakberichten via telefoon aan deelnemers
- Preventief/informatief bericht via e-mail aan deelnemers
- Digitaal Buurtonderzoek via e-mail aan deelnemers
- Nieuwsbrief via e-mail aan deelnemers
- Bericht via digitale informatieborden (nog niet operationeel)

Door de Politie wordt gebruikgemaakt van bovenstaande kanalen. Daarbij zal bij de Politie de nadruk liggen op opsporing en bij de gemeenten op preventie. In de praktijk worden de sociale media ook door deelnemers zelf gebruikt, om een Burgernetbericht naar hun netwerk door te zetten. Door de gemeente wordt alleen gebruikgemaakt van van een preventieve/informatieve e-mail of een nieuwsbrief per e-mail.

Via Google Firebase wordt een beperkt aantal gebruikersacties geregistreerd door middel van trigger in de app. Deze trigger is het voor de eerste keer openen van de app.

Onderstaand volgt een nadere toelichting op de functionele werkwijzen van Burgernet.

3.2.2 Burgernetserver

De Burgernetserver[4] draait in het datacenter van de Politie en bestaat uit de volgende onderdelen:

- beheerportaal
- actieportaal
- dashboard

[4] Voor een overzicht wordt verwezen naar bijlage 4

Beheerportaal
Het functioneel beheer van de Burgernetserver, de Burgernetapplicatie en koppelingen ligt bij Landelijk Functioneel Beheer Burgernet onder aansturing van de Stuurgroep Burgernet. Het beheer wordt uitgevoerd via het beheerportaal. De landelijke beheerders geven ook autorisaties voor het kunnen uitzetten van acties (meldkamers) en toegang tot het actieportaal, beheerportaal en dashboard. Er is geen schriftelijke procedure voor het aanmelden van nieuwe gemeentelijke beheerders.

Actieportaal
Via het actieportaal verstuurt de Politie buurtonderzoeken per e-mail. Preventieve berichten en nieuwsbrieven worden door de gemeenten per e-mail verstuurd. De meldingen die binnenkomen in reactie op een e-mail van de Politie worden via het Burgernet systeem door de Politie verwerkt. Voor gemeenten is er een mogelijkheid om via het actieportaal nieuwsbrieven te versturen. Het bericht wordt dan door de gemeente klaargezet en via het actieportaal zelf verstuurd. De gemeente heeft daarbij geen toegang tot de (persoons)gegevens in de database.

Dashboard
In het dashboard worden aantallen deelnemers, app gebruikers en Burgernetacties gegeven over deelnemers en (anonieme) appgebruikers (tijdkritisch en niet-tijdkritisch). Via het dashboard is zichtbaar hoe Burgernet functioneert in een gemeente. Er is te zien hoeveel deelnemers er in een gemeente zijn en of er sprake is van trends in het aantal aanmeldingen of downloads van de app. Ook het aantal en de aard van de Burgernetacties is zichtbaar, wat input kan geven voor het veiligheidsbeleid van een gemeente[5].

3.2.3 Deelnemersportaal en appserver
Naast de Burgernetserver is er ook een deelnemersportaal en een Burgernet appserver. Beide worden buiten het datacenter van de Politie gehost. Bij Intermax Cloudsourcing B.V wordt het deelnemersportaal gehost. Deze provider werkt conform ISO27001 en NEN 7510 waarvan is aangegeven dat auditrapporten beschikbaar zijn[6]. De reden voor het buiten het datacenter van de Politie hosten is dat het datacenter van de Politie niet berekend is op veel dataverkeer. Dat is wel het geval als er veel actieve gebruikerssessies zijn. Daarvan is bijvoorbeeld sprake als een promotieactie veel respons oplevert. Bij een promotieactie kan bijvoorbeeld worden gedacht aan het werven van nieuwe deelnemers door gemeenten, hetgeen een verantwoordelijkheid is van de gemeenten. De gegevens van deelnemers die zich hebben aangemeld via de website van Burgernet worden beheerd door de gemeente waarin de deelnemers hebben aangegeven woonachtig te zijn. Hiervoor is een handleiding beschikbaar[7]. In principe kan een deelnemer dit ook zelf via de website van Burgernet. De Burgernet app server wordt gehost door M2Mobi. In de verwerkersovereenkomst is een bepaling opgenomen dat de beveiligingsmaatregelen door de verwerker zullen worden beschreven en aan de opdrachtgever verstrekt. Dit document is niet bij de verwerkersovereenkomst gevoegd. Het is niet duidelijk of de verwerker dit document wel heeft opgesteld.

[5] Burgernet infobulletin Raadsleden Gemeente 2018
[6] Gelet op de scope van de opdracht zijn deze niet inhoudelijk beoordeeld.
[7] Relatiebeheer Burgernet 2.0

3.3 Processen

3.3.1 Aanmelden, afmelden en het doorgeven van wijzigingen als deelnemer van Burgernet via website

Aanmelden als deelnemer van Burgernet kan via het deelnemersportaal[8]. Van deelnemers worden locatie en contactgegevens geregistreerd: telefoonnummer, postcode en huisnummer en e-mailadres. Het e-mailadres wordt ook gebruikt om de aanmelding te verifiëren. Deelnemers ontvangen een spraak- of sms-bericht, of Twitter, of Burgernet app bericht of een bericht via Facebook messenger als er iets gebeurt in de omgeving van de deelnemer. Via een speciaal telefoonnummer kan dan direct naar de juiste meldkamer van de Politie worden gebeld of direct via 112. Er kan via dat nummer niet anoniem naar de meldkamer van de Politie worden gebeld. Anoniem bellen naar aanleiding van een actie kan wel naar het telefoonnummer van Meld Misdaad Anoniem.

Via het deelnemersportaal kunnen deelnemers hun gegevens beheren en kunnen zij zich eventueel ook weer uitschrijven. Het beheer van de gegevens van de deelnemers is in beginsel de verantwoordelijkheid van de deelnemers zelf.

Ook kan er een contactformulier worden ingevuld voor het stellen van vragen of het doen van verzoeken, zoals bijvoorbeeld het afmelden van iemand die overleden is. Op het contactformulier moet de naam van de gemeente worden ingevuld, zodat de vraag kan worden voorgelegd aan de gemeente waarin zij dan wel de overledene wonen. Het verwerken van deze mutaties van deelnemers is in deze gevallen de verantwoordelijkheid van de gemeenten.

De autorisaties hiervoor worden uitgegeven door de regionaal functioneel beheerders van de Politie of de landelijk functioneel beheerder.

Er is sprake van reactief beheer: De wijzigingen die de deelnemers doorgeven, zoals bijvoorbeeld adreswijzigingen, worden op verzoek verwerkt in het systeem. Gemeenten voeren geen actief beheer om de gegevens up-to-date te houden. Er wordt dus geen informatie ontleend aan de Basis Registratie Personen (BRP).

3.3.2 Aanmelden, afmelden en het doorgeven van wijzigingen als deelnemer van Burgernetapp

Behalve via het aanmelden via de website, kan een deelnemer ook gebruik-maken van een app. Deze app is gratis te downloaden via de Appstore (voor Apple-telefoons) of Googleplay (voor Android-telefoons). Voor de deelname kan aan de app toestemming worden gegeven voor het gebruik van de locatie, maar dit is optioneel. Er kunnen ook een of meerdere gebied(en) en een straal (aantal km) worden aangemaakt waarvoor de deelnemer berichten wil ontvangen. Dat is dus ongeacht zijn feitelijke locatie. Welke gebieden dit zijn wordt niet centraal opgeslagen. Bij aanmelding is het verstrekken van (aanvullende) persoonsgegevens niet nodig, tenzij er wordt deelgenomen aan digitaal buurtonderzoek. In dat geval worden een e-mailadres, postcode en huisnummer gevraagd.

[8] via www.burgernet.nl

Het LPB noch de Politie weet wie, of hoeveel personen zich voor bepaalde gebieden hebben aangemeld. De Burgernetapp vraagt op het device, naast locatie, ook toestemming voor toegang tot foto's/media/bestanden en camera. Hierdoor is de gebruiker in staat om via de app ook beeldmateriaal aan te leveren. Burgernet krijgt alleen beschikking over de gegevens die worden verzonden door de gebruiker, maar heeft zelf geen toegang tot de camera.

De Burgernetapp checkt periodiek of er nieuwe berichten klaarstaan. Als dit het geval is krijgt de Burgernet app server een token van het device inclusief locatie, waarmee de server een pushbericht met daarin de inhoud van het bericht naar het device stuurt. Dit token wordt eenmalig gebruikt en blijft niet bewaard. Gemeenten en de Politie hebben geen toegang tot deze informatie. De app toont alleen de berichten die vallen binnen de door de gebruiker aangegeven gebieden. Op het device worden geen berichten opgeslagen. Bij het openen van de Burgernetapp worden de berichten steeds opnieuw geladen.

De provider van de app is In-Pact B.V op basis van informatie in de app zelf. Het LPB heeft aangegeven dat dit M2Mobi moet zijn. In de app zelf is geen informatie over de provider beschikbaar. Wel is er over het privacybeleid van de Burgernetapp informatie beschikbaar waarbij wordt doorgelinkt naar het privacybeleid van Burgernet. In dit privacybeleid is verwoord dat er geen persoonsgegevens nodig zijn voor het gebruik van de app en dat er geen locatiegegevens worden opgeslagen die te herleiden zijn naar de telefoon van de gebruiker.

3.3.3 Uitsturen Burgernet-actiebericht

Als door de centralist van de meldkamer van de Politie wordt besloten tot het inzetten van een Burgernetmelding, dan worden de volgende processtappen onderscheiden:

- bepalen of een actie kan worden uitgezet;
- opstellen tekst;
- inspreken spraakbericht en opstellen sms-bericht;
- selecteren gebied;
- uitsturen.

Via de Burgernetapp, Twitter en Facebook Messenger wordt hetzelfde bericht verspreid. Dit bericht wordt ook gepubliceerd op de website.

Als een burger via de Burgernetapp contact zoekt met de meldkamer, hangt de werking af van het Operating System (OS):

- IOS: vanuit de Burgernetapp wordt meegegeven voor welke actie wordt gebeld zodat er direct naar de juiste meldkamer wordt doorverbonden.
- Op Android-telefoons werkt dit niet. De beller komt dan binnen op 112, waar vervolgens wordt doorgezet naar de juiste regionale meldkamer.

Er zijn drie verschillende berichttypen: een startbericht, een uitbreidingsbericht en een afloopbericht. Alle berichten blijven in Burgernet staan.

In enkele gevallen worden berichten later aangepast: er kan ook een verwijderverzoek worden ingediend. Burgernet dient dan ook verzoeken in bij Google om de berichten daar te verwijderen.

3.3.4 Digitaal buurtonderzoek/nieuwsbrief

Het digitaal buurtonderzoek wordt door de Politie ingezet als opsporingsmiddel achteraf. Een dergelijk verzoek wordt uitgezet via e-mail. Digitale buurtonderzoeken worden aangevraagd: naast de persoon die het onderzoek aanvraagt en in het systeem zet, moet een ander het verzoek goedkeuren.

Burgers kunnen reageren via een webportal dat staat in de Burgernet-serveromgeving in het Politie datacenter (opsporingsgegevens). De respons kan alleen worden gelezen door de verzender van het bericht.

Preventieve berichten en nieuwsbrieven worden verzonden door de gemeenten. Gemeenten zijn vrij in de wijze waarop zij binnen hun interne organisatie het akkoord op de inzet en tekst vormgeven.

3.4 Aspecten van informatiebeveiliging en uitwerking van informatie beveiligingsvoorschriften

Uit de gesprekken blijkt dat de beveiliging van Burgernet zowel bij de Politie als binnen het programma Burgernet veel aandacht krijgt. Over de beveiliging van gegevens die worden verwerkt in het kader van Burgernet zijn afspraken gemaakt tussen het programmabureau en de Politie. Dit betreft de verwerking van persoonsgegevens zoals beschreven in bijlage 3. De gemaakte afspraken zijn vastgelegd in het Dossier Afspraken en Procedures (DAP). Deze afspraken zijn in het kader van deze rapportage beoordeeld. Tijdens de interviews is aangegeven dat de gegevens die worden verwerkt binnen de technische infrastructuur van de Politie, worden beveiligd volgens de normen zoals die gelden voor de beveiliging van politiegegevens[9]. Hieronder vallen technische eisen, maar ook voorschriften ten aanzien van het toekennen en intrekken van autorisaties, logging van alle systeem toegang, lees- en schrijfactiviteiten en de actieve monitoring daarvan. Bij het toekennen van autorisaties worden de bij de Politie gebruikelijke procedures gevolgd. Dit betekent onder andere dat applicatiebeheerders van CGI zijn gescreend volgens de normen die gelden voor de informatiesystemen van de Politie. Voor de borging van de beveiligingsvoorschriften is door de Politie een security officer is aangesteld.

De security officer van de Politie is verantwoordelijk voor de technische infrastructuur bij de Politie, waaronder de Burgernetserver die wordt gehost in het datacenter van de Politie. De volledige Burgernet-infrastructuur bestaat echter ook uit de Burgernet app server en het deelnemersportaal. Uit de gesprekken blijkt niet wie de borging van de beveiliging van dit deel van de Burgernet-infrastructuur tot zijn taak rekent[10]. De websites worden buiten de politieomgeving gehost. Het sms-verkeer lift mee op de raamovereenkomst die de Politie heeft met de provider.

[9] Deze zijn onder andere te vinden in de Wet Politiegegevens, Besluit Politiegegevens en de Regeling Informatiebeveiliging Politie
[10] Binnen het programma Burgernet is er geen security officer aangesteld

Hoofdstuk 4 Bevindingen

4.1 Verantwoordelijk voor de gegevensverwerking

Voor de verwerking van persoonsgegevens bij de toepassing van Burgernet is het van belang vast te stellen wie als verantwoordelijke is aan te duiden voor de gegevensverwerking. Daarvoor kan worden gekeken naar de feitelijke en juridische situatie.

Voor de feitelijke situatie wordt verwezen naar hoofdstuk 3. In dit hoofdstuk is een beschrijving gegeven van de huidige werkwijze van Burgernet. Uit deze beschrijving blijkt dat de technische infrastructuur waarmee Burgernet wordt beheerd en toegepast valt onder de verantwoordelijkheid van de Politie. Dit blijkt onder meer uit de afspraken die zijn gemaakt met leveranciers. In deze overeenkomsten[11] treedt de Politie op als verwerkingsverantwoordelijke.

Voor het bepalen van de juridische situatie is het van belang te beoordelen welk wettelijk kader van toepassing is. Daarvoor is het noodzakelijk om vast te stellen vanuit welk doel de inzet van Burgernet plaatsvindt. Uit de geanalyseerde documenten blijkt dat er meerdere vormen van inzet kunnen zijn. Onderstaande geldt bij aanmelding voor Burgernet via de website van Burgernet en de Burgernetapp.

De primaire inzet van Burgernet is gericht op de uitvoering van de politietaak[12]. Het betreft dan situaties waarin er sprake is van bijvoorbeeld vermissing, diefstal, een overval of een verdachte situatie. In dat geval kan een *Burgernet alert* worden uitgedaan[13]. Ook kan er sprake zijn van *digitaal buurtonderzoek*. In dat laatste geval wordt in het kader van opsporing achteraf aan de deelnemers rond een bepaalde locatie informatie gevraagd. Zij ontvangen op het opgegeven e-mailadres een bericht[14].

Daarmee is er sprake van het verwerken van persoonsgegevens voor het uitvoeren van de politietaak. Op grond van de Wpg is de Korpschef van de Politie hiervoor verantwoordelijk[15]. Gelet op de feitelijke en juridische situatie kan worden geconcludeerd dat de Politie kan worden aangemerkt als verwerkingsverantwoordelijke onder de Wpg. Het betreft dan de verwerking van persoonsgegevens van deelnemers in het kader van de deelname aan Burgernet door aanmelding via de website of de Burgernetapp.

Naast de primaire taak in het kader van opsporing door de Politie bestaat er ook de mogelijkheid voor gemeenten om *nieuwsbrieven en preventieve berichten* te versturen.

---

[11] Dit betreft de verwerkersovereenkomsten met M2Mobi en Intermax Cloudsourcing
[12] Artikel 3 Politiewet
[13] https://www.burgernet.nl/about
[14] Indien betrokkene valt binnen de geografische reikwijdte op basis van zijn adres.
[15] Op grond van artikel 3 Politiewet (taak), artikel 1 onder a en b Wet politiegegevens (persoonsgegeven voor de uitvoering van de Politietaak) en artikel 1 onder f Wet politiegegevens (verantwoordelijke)

In dat geval wordt naar een bepaalde gemeente, postcode of geo-gebied een bericht verstuurd met algemene informatie over de veiligheidheid in een wijk of plaats. Hierbij kan worden gedacht aan het het beheer van woningen tijdens de vakantieperiode of het niet zichtbaar achterlaten van waardevolle voorwerpen in auto's. Deze taak past binnen de verantwoordelijkheid voor de openbare orde binnen een gemeente[16] en het veelal daarop gebaseerde preventieve veiligheidsbeleid.

Indien een gemeente van deze mogelijkheid gebruik wil maken, dan kan een gemeente de tekst en de geografische reikwijdte aangeven via het actieportaal. De gemeente kan in dit geval niet zien aan wie het bericht wordt verstuurd, maar is wel verantwoordelijk voor het versturen van het bericht. Er wordt door de Politie geen inhoudelijke toets uitgevoerd op het bericht en er wordt ook geen formeel akkoord gegeven voor de verzending. Daarmee kan worden bepleit dat voor dit doel van de gegevensverwerking een individuele gemeente de verwerkingsverantwoordelijke is onder de AVG.

Daarmee is in die situatie, afhankelijk van het doel waarvoor de gegevens worden gebruikt, een verschillend wettelijk regime van toepassing voor dezelfde gegevens. Bijvoorbeeld het gebruik van de e-mailadressen (digitaal buurtonderzoek - Politie - Wpg of nieuwsbrief - gemeente - AVG).

Vanuit het perspectief van zowel de betrokkene als gemeenten en Politie is dit geen wenselijke situatie. Het kan bijvoorbeeld onduidelijkheid geven ten aanzien van het uitoefenen van rechten van betrokkenen. De Wpg kent daarbij andere bepalingen dan de AVG. Ook kunnen er verschillen bestaan in het niveau van beveiliging, onduidelijkheid over het doen van datalekmeldingen, het aanstellen van een Functionaris Gegevensbescherming en het verplicht uitvoeren van audits.

Op basis van bovenstaande is de conclusie gerechtvaardigd dat de Politie de verwerkingsverantwoordelijke is voor de verwerkingen in het kader van Burgernet. Dit doet recht aan het feit dat de Politie de verwerkersovereen-komsten met CGI, M2Mobi en Intermax Cloudsourcing ook reeds als verwerkingsverantwoordelijke is aangegaan. Ook past dit binnen het belangrijkste en meest zichtbare onderdeel van Burgernet, namelijk opsporing. Het feit dat de Politie optreedt als verwerkingsverantwoordelijke doet overigens geen afbreuk aan de bestaande afspraak dat gemeenten verantwoordelijkheid dragen voor het beheer van deelnemergegevens. Vanuit het belang dat gemeenten hebben bij actuele gegevens van hun eigen inwoners in het kader van hun preventieve veiligheidsbeleid is dit verklaarbaar. Op grond van artikel 172 Gemeentewet heeft de burgemeester de mogelijkheid om preventieve berichten of nieuwsbrieven te versturen aan inwoners van zijn gemeente gericht op openbare orde en veiligheid.

Gelet op de verantwoordelijkheid van de Politie voor de verwerkingen op grond van de Wpg betekent dit dat de bestaande afspraken in dat licht moeten worden getoetst en waar nodig aangevuld of gewijzigd.

[16] Op basis van artikel 172 Gemeentewet

Hierbij kan bijvoorbeeld worden gedacht aan afspraken over beveiliging, datalekken, beheer van gegevens (waaronder rechten van betrokkenen) en toegang tot gegevens.

Ten aanzien van de rol van het LPB is vastgesteld dat het geen rechtspersoonlijkheid heeft en ook de positie en formele verantwoordelijkheden en de relatie tot de Politie en gemeente(n) niet transparant zijn beschreven of vastgelegd. Aanbevolen wordt om voor de betrokken partijen alsook voor deelnemers aan burgernet de rol en positie te beschrijven.

Conclusie: de Politie treedt feitelijk op als (Wpg) verwerkingsverantwoordelijke in het kader van Burgernet door het afsluiten van verwerkingsovereenkomsten. Het betreft dan de verwerking van persoonsgegevens van deelnemers in het kader van de deelname aan Burgernet door aanmelding via de website en Burgernetapp. Daarnaast is de Politie voor de primaire functie van Burgernet ook juridisch gezien te beschouwen als verwerkingsverantwoordelijke. Kleinere onderdelen van de verwerkingen in het kader van Burgernet zijn uitbesteed aan gemeenten. Dit leidt tot onduidelijkheden over verantwoordelijkheden en toepasselijk juridisch kader welke in de praktijk kunnen leiden tot onduidelijkheden voor zowel de deelnemende partijen als voor de individuele betrokkenen.

Aanbeveling: Ga bij de verwerking van persoonsgegevens in het kader van Burgernet uit van een verwerkingsverantwoordelijkheid van de Politie op grond van de Wpg. Toets op basis daarvan de bestaande afspraken en pas waar nodig deze aan. Hierbij kan bijvoorbeeld worden gedacht aan afspraken over beveiliging, datalekken, beheer van gegevens (waaronder rechten van betrokkenen) en toegang tot gegevens.

Conclusie: de positie en formele verantwoordelijkheden van het LPB en de relatie tot de Politie en gemeente(n) zijn niet transparant beschreven of vastgelegd.

Aanbeveling: beschrijf voor de betrokken partijen alsook voor deelnemers aan Burgernet de rol en positie van het LPB.

4.2 Verwerking van persoonsgegevens

De Wpg is van toepassing als er sprake is van het verwerken van persoons-gegevens in het kader van de uitoefening van een politietaak[17]. Persoonsgegevens zijn in de Wpg[18] gedefinieerd als:

> *Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.*

Zoals in de vorige paragraaf is geconstateerd wordt van deelnemers die zich hebben aangemeld voor Burgernet *via de website* het telefoonnummer, e-mail, postcode en huisnummer vastgelegd.

[17] Artikel 1 onder a Wpg
[18] Artikel 1 onder b Wpg

Het begrip persoonsgegeven uit de Wpg gaat uit van alle alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Op basis van een telefoonnummer kan in principe al worden gesproken van een persoonsgegeven.

Door middel van een telefoonnummer is voor de Politie een abonnementhouder te achterhalen en daarmee is de betrokkene identificeerbaar. Maar ook indien dat niet het geval is, bijvoorbeeld in het geval van een prepaid- telefoon, dan is de postcode en het huisnummer en/of het e-mailadres ook voldoende voor het identificeren van een natuurlijk persoon. Daarmee kan worden gesteld dat deze set van gegevens kan worden beschouwd als een persoonsgegeven in het kader van de Wpg[19]. Voor een volledig overzicht van persoonsgegevens wordt verwezen naar bijlage 3.

Ook de gegevens die worden verwerkt bij gebruik van de Burgernetapp, indien de gebruiker zich aanmeldt voor het digitaal buurtonderzoek, zijn persoonsgegevens. Daarmee zijn dit ook persoonsgegevens op grond van de Wpg.

Conclusie: In het kader van Burgernet worden persoonsgegevens verwerkt. Dit betreft zowel de gegevens bij aanmelding via de website als bij gebruikmaking van de Burgernetapp.

4.3 Rechtmatigheid van de verwerking en noodzaak

Op basis van de vorige paragrafen is vastgesteld dat de Politie als verwerkingsverantwoordelijke kan worden gezien voor de verwerking van persoonsgegevens in het kader van Burgernet. De verwerking valt onder de Wpg. Voor het verwerken van deze persoonsgegevens is het van belang dat deze verwerking noodzakelijk en rechtmatig is.

Op grond van de Wpg worden politiegegevens slechts verwerkt voor zover dit noodzakelijk is voor de bij deze wet geformuleerde doeleinden[20]. Een van deze doeleinden kan zijn de uitvoering van de dagelijkse politietaak[21]. Onder de dagelijkse politietaak verstaat de Politie het dagelijks politietoezicht door agenten op straat, in het verkeer en in de wijken. Zij zorgen voor een veilige en leefbare wijk, stad of regio door politietoezicht, preventieadvies, afhandeling van verkeersproblemen, eenvoudig recherchewerk, verlenen van hulp en het handhaven van wetten en regels[22]. De opsporing en nieuwsberichten, gericht op preventie zoals dat in het kader van Burgernet plaatsvindt, kwalificeert zich daarmee als dagelijkse politietaak.

De persoonsgegevens van de deelnemers aan Burgernet die worden verwerkt ter uitvoering van de dagelijkse politietaak zijn telefoonnummer, e-mailadres en postcode en huisnummer.

---

[19] Het is mogelijk dat de set van gegevens niet te herleiden is naar een natuurlijk persoon. Bijvoorbeeld in het geval van een prepaid telefoon, een onjuist of niet bestaand adres en een niet te herleiden mailadres. Het merendeel van de aanmelders zal op basis van de aangeleverde gegevens echter identificeerbaar zijn.
[20] Artikel 3 Wet politiegegevens
[21] Artikel 8 Wet politiegegevens
[22] Zie https://www.politie.nl/themas/politietaken.html

Deze gegevens worden gebruikt om de deelnemers als potentiële getuigen te kunnen benaderen in het kader van opsporing of in het kader van preventie met behulp van Burgernet. Met het telefoonnummer en e-mailadres kan de deelnemer van Burgernet worden bereikt en met het adres kan worden beoordeeld *welke* deelnemer wordt benaderd.

Voornoemde verwerking kan daarmee als noodzakelijk worden beschouwd. Op deze wijze kunnen in tijdkritische situaties snel potentiële getuigen worden geselecteerd en benaderd in het kader van de dagelijkse politietaak. Ook in het kader van de preventieve taak kunnen met behulp van deze gegevens de juiste deelnemers worden benaderd in een bepaalde regio of wijk waarin preventie is aangewezen.

Daarnaast is het op grond van de Wpg van belang dat de verwerking behoorlijk en rechtmatig is, de gegevens rechtmatig zijn verkregen en de gegevens, gelet op de doeleinden waarvoor zij worden verwerkt, toereikend, terzake dienend en niet bovenmatig zijn[23].

Voor de beoordeling hiervan is het van belang dat in het kader van de rechtmatigheid de gegevens door de deelnemers vrijwillig worden verstrekt. Er is op geen enkele wijze een verplichting voor deelnemers om mee te doen met Burgernet. Indien deelnemers dat wensen, kunnen zij eenvoudig hun deelname aan Burgernet beëindigen en worden de persoonsgegevens verwijderd uit de bestanden bij de Politie. Informatie over de werkwijze van Burgernet en de betrokken partijen zijn beschikbaar op de website van Burgernet.

Zoals bovenstaand toegelicht zijn de verwerkte gegevens noodzakelijk voor de toepassing van Burgernet. Uit de interviews blijkt dat de gegevens alleen worden gebruikt voor het selecteren en benaderen van potentiële getuigen of in het kader van preventie. Voor deze doeleinden wordt een minimale set aan gegevens verwerkt. Deze gegevens zijn toereikend, terzake dienend en niet bovenmatig. Op grond hiervan kan de verwerking als behoorlijk worden beschouwd.

Bij het gebruik van de Burgernetapp worden in principe maximaal dezelfde persoonsgegevens verwerkt op basis van een vergelijkbare werkwijze. Daarmee geldt de conclusie ten aanzien van de rechtmatigheid en noodzaak ook voor de verwerking van persoonsgegevens in de Burgernetapp.

Conclusie: de verwerking van persoonsgegevens door de Politie in het kader van Burgernet kan op basis van bovenstaande als voldoende noodzakelijk en rechtmatig worden beschouwd.

[23] Artikel 3 Wet politiegegevens

4.4 Risico's voor de rechten en vrijheden van betrokkenen en waarborgen

4.4.1 Inleiding

Zoals onder paragraaf 4.2 is geconcludeerd, is er bij de gegevens die worden verwerkt bij de aanmelding via de website van Burgernet sprake van persoonsgegevens.
In paragraaf 4.3 is geconcludeerd dat de Politie voor het verwerken van de persoonsgegevens een rechtmatige grondslag heeft en dat niet is vastgesteld dat de gegevens bovenmatig zijn. Voor de Burgernetapp geldt een gelijkluidende conclusie.

In paragraaf 4.1 is geconcludeerd dat op de verwerking van persoonsgegevens in het kader van Burgernet de Wpg van toepassing is. Daarbij gaat het om deelnemers die vrijwillig persoonsgegevens beschikbaar stellen voor deelname.

4.4.2 Transparantie

In de Wpg zijn een aantal bepalingen opgenomen die betrekking hebben op transparantie. Dit betreft onder meer de identiteit en contactgegevens van de verwerkingsverantwoordelijke en de Functionaris Gegevensbescherming (FG), de verwerkingsdoeleinden en de rechten van betrokkenen[24].

Burgernet heeft een eigen website waar burgers zich kunnen aanmelden als deelnemer. Op deze website is veel informatie te vinden over wat Burgernet is, de werking van Burgernet en hoe wordt omgegaan met persoonsgegevens. Deze informatie is voor de deelnemers kort weergegeven in de vorm van vraag en antwoord. Daarmee is Burgernet transparant over het functioneren van Burgernet en welke gegevens worden verwerkt.

Op de website van Burgernet[25] is geen informatie te vinden over de identiteit van de verantwoordelijke. Er kan wel een contactformulier worden ingevuld waarbij wordt verwezen naar de gemeente van de deelnemer. Ook is op de website van Burgernet geen verwijzing te vinden naar een FG van de Politie. Ten aanzien van het uitoefenen van de rechten van betrokkenen is wel duidelijk aangegeven op welke wijze men zich kan afmelden voor deelname aan Burgernet of hoe men kan verzoeken om een actiebericht te verwijderen[26]. Daarmee is voldoende informatie beschikbaar voor het gebruik kunnen maken van het recht tot verwijdering. Over de overige rechten die een betrokkene heeft, bijvoorbeeld inzage, is geen informatie opgenomen. Gelet op het doel van Burgernet zal een dergelijk verzoek niet vaak voorkomen, maar volledigheidshalve is het vermelden van alle rechten op grond van de Wpg aangewezen. Overigens wordt op de website verwezen naar de Wet bescherming persoonsgegevens (Wbp). Deze wet is inmiddels niet meer van toepassing en is een verwijzing naar de Wpg aanbevolen.

[24] Artikel 24a en 24b Wpg
[25] www.burgernet.nl
[26] https://www.burgernet.nl/privacy

In de app is informatie beschikbaar over de werking van Burgernet, het gebruik van de gps-locatie van de telefoon en dat geen persoonsgegevens noodzakelijk zijn voor het gebruik van de app. Ook hier geldt dat geen contactgegevens beschikbaar zijn van de verantwoordelijke.

Conclusie: De beschikbare informatie op de website van Burgernet en in de app geeft inzicht in de werking van Burgernet en de verwerking van persoonsgegevens. De informatie is echter nog niet volledig. Er ontbreekt nog aanvullende informatie over de identiteit van de verwerkingsverantwoordelijke, de Functionaris Gegevensbescherming en de overige rechten van betrokkenen.

Aanbeveling: Vul de website van Burgernet en de informatie in de app aan met informatie over de identiteit van de verwerkingsverantwoordelijke, de Functionaris Gegevensbescherming en de overige rechten van betrokkenen. Vervang de verwijzing naar de Wbp door de Wpg.

4.4.3 Verwijderingstermijnen

Zoals in paragraaf 4.1 is aangegeven, wordt aanbevolen de Politie als verwerkingsverantwoordelijke te beschouwen voor de verwerkingen in het kader van Burgernet. De grondslag voor de verwerking kan worden gevonden in artikel 8 Wpg. Op grond van dit artikel kan de Politie persoonsgegevens in het kader van de dagelijkse politietaak verwerken. De activiteiten van Burgernet vallen onder de uitleg van de dagelijkse politietaak.

Op grond van artikel 8 Wpg mogen persoonsgegevens worden bewaard zolang deze noodzakelijk zijn en maximaal één jaar. Dit betekent dat de gegevens voor de aanmelding in dat geval niet langer dan een jaar mogen worden bewaard.

Voor de werking van Burgernet past een maximale bewaartermijn van één jaar van de gegevens van deelnemers echter niet bij de doelstelling van Burgernet. Het doel is een langdurige participatie van deelnemers bij Burgernet, als potentiële getuige, op basis van vrijwilligheid.

Het verlopen van de bewaartermijn kan relatief eenvoudig worden opgelost door middel van een jaarlijks e-mailbericht aan alle deelnemers. In dit bericht kan het doel van Burgernet opnieuw bij iedereen onder de aandacht worden gebracht (transparantiebeginsel). Met het e-mailbericht kan worden bereikt dat deelnemers zich formeel opnieuw inschrijven waarmee opnieuw een verwijderingstermijn van één jaar wordt aangevangen. Daarnaast kunnen deelnemers worden opgeroepen om tijdig gewijzigde adresgegevens en telefoonnummers door te geven via het gebruikersportaal. Hiermee kan worden voorkomen dat de gegevens verouderen (juistheidsbeginsel).

De gegevens die worden verwerkt in het kader van de app beperken zich tot locatiegegevens, die per keer ook weer worden verwijderd en de contactgegevens in het kader van deelname aan een digitaal buurtonderzoek. Daarbij blijven de contactgegevens niet achter in de app, maar wel op de Burgernet server. Ook deze verwerking valt onder de Wpg met een maximale bewaartermijn van een jaar. Aangezien niet op voorhand kan worden bepaald van wie de beperkte set aan gegevens in het kader van het digitale

buurtonderzoek noodzakelijk is, kan het bewaren van deze gegevens als noodzakelijk worden beschouwd.
Daarbij is ook relevant dat betrokkene zelf zijn gegevens kan verwijderen. Aangezien ook deze gegevens vallen onder de algemene politietaak, geldt ook hiervoor een maximale bewaartermijn van een jaar. Ook hier kan een jaarlijks bericht worden ingezet.

Conclusie: voor de verwerking van persoonsgegevens in het kader van Burgernet geldt bij aanmelding van de website of via de Burgernetapp op grond van artikel 8 Wpg een maximale bewaartermijn van één jaar.

Aanbeveling: Gelet op het doel van Burgernet is een maximale bewaartermijn van één jaar van deelnemersgegevens niet werkbaar. Om die reden wordt aanbevolen jaarlijks deelnemers te berichten over het hun deelname aan Burgernet met de mogelijkheid zich opnieuw in te schrijven en hun gegevens te actualiseren. Hiermee wordt ook het transparantie- en juistheidsbeginsel nageleefd.

Aandachtspunt is wel het verwijderen van afgesloten acties. Deze blijven beschikbaar op de website of Burgernetapp. Daarmee kan de functionaliteit van Burgernet worden aangetoond. Alhoewel de verwerkte gegevens in principe anoniem zijn, zijn deze vaak voor wijk of buurtbewoners te herleiden naar een individueel persoon, zeker bij vermissingen. Met name in het geval van kinderen wordt aanbevolen deze gegevens na sluiting van het actiebericht te verwijderen. Het verliest met het sluiten van het bericht de noodzaak tot verwerken. Daarbij komt dat met name kinderen op latere leeftijd alsnog kunnen worden geconfronteerd met hun vermissing.

Conclusie; Na sluiting van een actiebericht zijn gegevens over vermissing van kinderen niet langer noodzakelijk. Gelet op mogelijke confrontatie op latere leeftijd is tijdig verwijderen van deze gegevens aangewezen.

Aanbeveling: stel een korte termijn vast voor het verwijderen van gegevens van vermiste kinderen na sluiting van de actie.

4.4.4 Aspecten van informatiebeveiliging en uitwerking van informatie beveiligingsvoorschriften

In paragraaf 4.1 is opgemerkt dat de technische infrastructuur van Burgernet functioneert onder verantwoordelijkheid van de Politie. Dit blijkt onder meer uit de afgesloten verwerkersovereenkomsten waarin de Politie optreedt als verwerkingsverantwoordelijke. Voor de verwerking van deze persoonsgegevens zijn de beveiligingseisen gebaseerd op de Wpg van toepassing. In de interviews is aangegeven dat de Politie de verplichtingen hieruit naleeft en de naleving hiervan volgens reguliere procedures controleert.

Ten aanzien van de beveiliging van gegevens die worden verwerkt in het kader van Burgernet geldt dat daarover afspraken zijn vastgelegd in het DAP. De afspraken zijn vastgelegd in een tweetal documenten. Een document beschrijft de afspraken tussen Burgernet en de Dienst ICT van de Politie. Een tweede document beschrijft de afspraken met de CGI, de partij die de

Burgernet-applicatie beheert. Dit laatste document is in het kader van deze rapportage ontvangen en beoordeeld.

Uit de ontvangen documenten is niet af te leiden of en op welke wijze de Politie als verwerkingsverantwoordelijke ook concreet wordt betrokken bij de beveiligingsaspecten van het deelnemersportaal en de Burgernet app server: het deel van de Burgernet-infrastructuur dat niet wordt gehost in het datacenter van de Politie. Het is van belang dat de verdeling van verantwoordelijkheden niet alleen in de praktijk invulling heeft gekregen maar dat dit ook is gedocumenteerd. Hierbij kan bijvoorbeeld worden gedacht aan risicoanalyses en audits.

Conclusie: omdat niet alle verantwoordelijkheden in het kader van de werking van Burgernet voldoende zijn gedocumenteerd, bestaat er een risico dat beveiligingsmaatregelen onvoldoende aandacht krijgen.

Aanbeveling: betrek de security officer van de Politie bij het geheel van de processen in het kader van Burgernet, ook buiten de processen van de Politie en documenteer de verschillende verantwoordelijkheden.

4.4.5. Procedure uitgifte, wijziging en intrekking van autorisaties

Zoals in paragraaf 3.2 is beschreven, geven de landelijke beheerders autorisaties voor het kunnen uitzetten van acties (meldkamers) en toegang tot het actieportaal, beheerportaal en dashboard. Daarnaast geven regionale beheerders autorisaties aan gemeentelijke beheerders zodat deze mutaties kunnen doen in de adresgegevens van deelnemers aan Burgernet. Deze procedures zijn nog niet schriftelijk vastgelegd. Daarnaast is het van belang dat wordt beschreven in welke rol of hoedanigheid gemeenteambtenaren het beheer over de (politie)gegevens voeren. Weliswaar gaat het hier om een zeer beperkte set aan gegevens welke vrijwillig door deelnemers beschikbaar is gesteld en waarbij geen sprake is van bijzondere of gevoelige gegevens, formeel betreft het toegang tot een politiesysteem. Daarmee is een formeel grond nodig voor het rechtstreeks toegang geven tot de adresgegevens van deelnemers.

Conclusie: Doordat de procedures voor uitgifte, wijziging en intrekking van autorisaties niet zijn vastgelegd, bestaat het risico dat medewerkers van de meldkamer of van gemeenten toegang houden tot persoonsgegevens die zij niet nodig hebben voor hun functie, en dat zij in staat zijn acties te initiëren en/of nieuwsbrieven te versturen naar grote groepen deelnemers, waartoe zij niet (meer) bevoegd zijn.

Conclusie: doordat niet duidelijk de rol of hoedanigheid is benoemd op grond waarvan gemeente ambtenaren toegang hebben tot adresgegevens van deelnemers bestaat het risico dat een rechtsgrond hiervoor ontbreekt.

Aanbeveling: Actualiseer de procedures voor de uitgifte, wijziging en intrekking van autorisaties van alle autorisaties met betrekking tot Burgernet en leg deze procedures schriftelijk vast. Controleer daarnaast jaarlijks tijdens de interne audit steekproefsgewijs of de afspraken ten aanzien van in-, door- en uitstroom worden nageleefd.

Aanbeveling: Leg formeel vast in welke rol of hoedanigheid gemeente-ambtenaren toegang hebben tot de adresgegevens van de deelnemers en leg vast op welke formele rechtsgrond zij rechtstreeks toegang krijgen.

4.4.6 Juistheid van de gegevens

Personen die deelnemen aan Burgernet door aanmelding van de website van Burgernet leveren via het deelnemersportaal zelf hun gegevens aan en zijn ook zelf verantwoordelijk voor het actueel houden daarvan. Er is een reële kans dat deze gegevens in de praktijk toch snel verouderen. Dit geldt voor zowel de adresgegevens en de telefoonnummers. In de praktijk zal bij een wijziging van adres of telefoonnummer een deelnemer niet als eerste denken aan het actualiseren van deze gegevens binnen Burgernet. Er is geen reden om aan te nemen dat deelnemers jegens Burgernet een buitengewone punctualiteit aan de dag zullen leggen.

Met name ten aanzien van mobiele telefoonnummers kan dit op den duur leiden tot een onjuiste adressering. Nummers die niet meer in gebruik zijn worden na verloop van tijd opnieuw uitgegeven. Het is dus denkbaar dat er sms-berichten worden verzonden naar telefoonnummers die niet meer in gebruik zijn bij de personen die zich hebben aangemeld, maar op termijn wel worden uitgegeven aan anderen. Deelnemers zijn in principe zelf verantwoordelijk voor de juistheid van de door hen ingevulde gegevens en worden ook in de gelegenheid gesteld deze aan te (laten) passen. Daarnaast kan vanuit de eigen verantwoordelijkheid van de Politie voor de juistheid van de gegevens overwogen worden jaarlijks een herinnering te sturen aan de deelnemers met het verzoek de juistheid te controleren. Dit bericht kan eventueel worden gecombineerd met een bericht in verband met de bewaartermijn zoals bedoeld in paragraaf 4.4.3.

Conclusie: betrokkenen zijn onvoldoende accuraat in het actualiseren van hun eigen gegevens, waardoor op de lange termijn de gegevens steeds minder up-to-date zijn.

Aanbeveling: bericht deelnemers jaarlijks met een verzoek de juistheid van hun gegevens te controleren.

4.4.7 Privacy by Design

Een belangrijk uitgangspunt van de privacywetgeving is dat al bij het ontwerp van informatiesystemen, procedures en werkinstructies zoveel mogelijk rekening moet worden gehouden met de risico’s voor de privacy van betrokkenen. Dit beginsel wordt aangeduid met het begrip ‘Privacy by Design’.

Zoals uit hoofdstuk 3 blijkt, en ook in de gesprekken uitvoerig is toegelicht, is bij het ontwerp van Burgernet veel aandacht besteed aan privacywaarborgen. Er worden niet meer gegevens vastgelegd dan strikt noodzakelijk voor het kunnen uitvoeren van de processen. De Burgernetapp is zo ontworpen dat op anonieme wijze aan Burgernet kan worden deelgenomen. De tokens die worden gebruikt om pushberichten naar de devices te kunnen sturen gelden wel als ‘persoonsgegeven’, omdat de tokens in beginsel kunnen worden herleid tot een specifieke telefoon, en daarmee ook tot een persoon. Deze tokens worden echter niet bewaard, maar worden per alert opnieuw gegenereerd. Door deze werkwijze wordt invulling gegeven aan het ‘Privacy by Design’ beginsel.

4.4.8 Verwerkersovereenkomst

De Politie heeft als verwerkingsverantwoordelijke drie verwerkers ingeschakeld. Dit zijn M2MOBI, CGI en Intermax Cloudsourcing. In de overeenkomsten zijn onder andere afspraken gemaakt over de vertrouwelijkheid van de gegevens, teruggave bij beëindiging, aansprakelijkheid en het melden van beveiligingsincidenten.

Naast de verwerkingen die onderdeel uitmaken van de technische infrastructuur van de Politie, vinden er ook enkele verwerkingen plaats buiten deze infrastructuur. Dit heeft te maken met de beschikbare capaciteit op het netwerk. Het betreft het deelnemersportaal en de Burgernet app server. Voor deze verwerkingen gelden de eisen die gelden voor het beveiligen van persoonsgegevens op grond van de Wpg.

Een korte beschouwing van de overeenkomst geeft als beeld dat alle onderwerpen die overeenkomstig de AVG in een verwerkersovereenkomst moeten worden geregeld, zijn opgenomen. In sommige gevallen wordt daarbij verwezen naar de hoofdovereenkomst welke in het kader van de rapportage niet zijn beoordeeld. In alle drie de verwerkersovereenkomsten zijn ook bepalingen opgenomen over de beveiliging van de persoonsgegevens. Ook dit vormt een verplicht onderdeel van een verwerkersovereenkomst. Daarbij wordt wel opgemerkt dat de opgenomen bepalingen algemeen zijn geformuleerd. Bijvoorbeeld dat passende technische en organisatorische maatregelen ten uitvoer worden gelegd. Dit is onvoldoende concreet om gezamenlijk een eenduidig beeld te hebben welke maatregelen dit zijn en tot welk niveau. In een andere overeenkomst wordt dit specifieker gemaakt door te verwijzen naar ISO27001 en NEN 7510. Dit zijn algemeen erkende en meer specifieke normen. Ook deze normen vragen echter vaak nog een nadere uitwerking. Aandachtspunt verder dat in die overeenkomst ook is bepaald dat het aan de opdrachtgever is zich ervan te verzekeren dat opdrachtnemer voldoet aan de beveiligingseisen voordat hij tot verstrekking overgaat. Daarmee lijkt de verantwoordelijkheid voor de gevolgen van beveiligingsincidenten bij de opdrachtgever te komen liggen.

Aanbevolen wordt om de huidige afspraken over de beveiliging aan een andere beschouwing te onderwerpen met inachtneming van bovenstaande aandachtspunten. Met name is daarbij van belang dat de normen voor de beveiliging voldoende beschreven en concreet zijn. Hierbij kan gebruikgemaakt worden van internationaal erkende normen. Indien de uitkomsten daartoe aanleiding geven, is bespreken met de verwerker(s) aangewezen.

Conclusie: omdat afspraken over de beveiliging onvoldoende concreet zijn, bestaat het risico dat daarmee onduidelijkheid ontstaat over de na te leven norm en daarmee persoonsgegevens onvoldoende beveiligd zijn.

Aanbeveling: onderwerp de huidige afspraken over beveiliging aan een nadere beschouwing en indien de uitkomsten daartoe aanleiding geven, bespreek deze met de verwerker(s).

4.4.9 Beveligingsincidenten en datalekken

De verwerking van persoonsgegevens in het kader van Burgernet valt onder de verwerkingsverantwoordelijkheid van de Politie. Op grond van artikel 33a Wpg is de Politie verplicht datalekken te melden bij de Autoriteit Persoonsgegevens. Hiervoor is bij de Politie een procedure beschikbaar welke ook betrekking heeft op het gebruik van Burgernet. Uit de interviews zijn geen relevante datalekken naar voren gekomen bij de uitvoeren van werkzaamheden binnen Burgernet.

Hoofdstuk 5 Conclusies en aanbevelingen

5.1 Conclusies en aanbevelingen

Op basis van deze DPIA zijn de volgende conclusies en aanbevelingen naar voren gekomen:

1. **Conclusie***:* de Politie treedt feitelijk op als (Wpg) verwerkingsverantwoordelijke in het kader van Burgernet door het afsluiten van verwerkingsovereenkomsten. Het betreft dan de verwerking van persoonsgegevens van deelnemers in het kader van de de deelname aan Burgernet door aanmelding via de website en Burgernetapp. Daarnaast is de Politie voor de primaire functie van Burgernet ook juridisch gezien te beschouwen als verwerkingsverantwoordelijke. Kleinere onderdelen van de verwerkingen in het kader van Burgernet zijn uitbesteed aan gemeenten. Dit leidt tot onduidelijkheden over verantwoordelijkheden en toepasselijk juridisch kader welke in de praktijk kunnen leiden tot onduidelijkheden voor zowel de deelnemende partijen als individuele betrokkenen.
   Aanbeveling*:* Ga bij de verwerking van persoonsgegevens in het kader van Burgernet uit van een verwerkingsverantwoordelijkheid van de Politie op grond van de Wpg. Toets op basis daarvan de bestaande afspraken en pas waar nodig deze aan. Hierbij kan bijvoorbeeld worden gedacht aan afspraken over beveiliging, datalekken, beheer van gegevens (waaronder rechten van betrokkenen) en toegang tot gegevens.

2. **Conclusie***:* de positie en formele verantwoordelijkheden van het LPB en de relatie tot de Politie en gemeente(n) zijn niet transparant beschreven of vastgelegd.
   Aanbeveling*:* beschrijf voor de betrokken partijen alsook voor deelnemers aan burgernet de rol en positie van het LPB.

3. **Conclusie***:* In het kader van Burgernet worden persoonsgegevens verwerkt. Dit betreft zowel de gegevens bij aanmelding via de website als bij gebruikmaking van de Burgernetapp.
   Aanbeveling: geen aanbeveling noodzakelijk.

4. **Conclusie***:* de verwerking van persoonsgegevens door de Politie in het kader van Burgernet kan op basis van bovenstaande als voldoende noodzakelijk en rechtmatig worden beschouwd.
   Aanbeveling*:* geen aanbeveling noodzakelijk.

5. **Conclusie***:* De beschikbare informatie op de website van Burgernet en in de app geeft inzicht in de werking van Burgernet en de verwerking van persoonsgegevens. De informatie is echter nog niet volledig. Er ontbreekt nog aanvullende informatie over de identiteit van de verwerkingsverantwoordelijke, de Functionaris Gegevensbescherming en de overige rechten van betrokkenen.
   Aanbeveling*:* Vul de website van Burgernet en de informatie in de app aan met informatie over de identiteit van de verwerkingsverantwoordelijke, de Functionaris Gegevensbescherming en de overige rechten van betrokkenen. Vervang de verwijzing naar de Wbp door de Wpg.

6. **Conclusie***:* voor de verwerking van persoonsgegevens in het kader van Burgernet geldt bij aanmelding van de website of via de Burgernetapp op grond van artikel 8 Wpg een maximale bewaartermijn van één jaar.
   Aanbeveling*:* Gelet op het doel van Burgernet is een maximale bewaartermijn van één jaar van deelnemersgegevens niet werkbaar. Om die reden wordt aanbevolen jaarlijks deelnemers te berichten over het hun deelname aan Burgernet met de mogelijkheid zich opnieuw in te schrijven en hun gegevens te actualiseren. Hiermee wordt ook het transparantie en juistheid beginsel nageleefd.

7. **Conclusie***;* Na sluiting van een actiebericht is zijn gegevens over vermissing van kinderen niet langer noodzakelijk. Gelet op mogelijke confrontatie op latere leeftijd, is tijdig verwijderen van deze gegevens aangewezen.
   Aanbeveling*:* stel een korte termijn vast voor het verwijderen van gegevens van vermiste kinderen na sluiting van de actie.

8. **Conclusie***:* Omdat niet alle verantwoordelijkheden in het kader van de werking van Burgernet voldoende zijn gedocumenteerd bestaat er een risico dat beveiligingsmaatregelen onvoldoende aandacht krijgen.
   Aanbeveling*:* betrek de security officer van de Politie bij het geheel van de processen in het kader van Burgernet, ook buiten de processen van de Politie en documenteer de verschillende verantwoordelijkheden.

9. **Conclusie***:* Doordat de procedures voor uitgifte, wijziging en intrekking van autorisaties niet zijn vastgelegd bestaat het risico dat medewerkers van de meldkamer of van gemeenten toegang houden tot persoonsgegevens die zij niet nodig hebben voor hun functie en dat zij in staat zijn acties te initiëren en/of nieuwsbrieven te versturen naar grote groepen deelnemers waartoe zij niet (meer) bevoegd zijn.
   Aanbeveling*:* Actualiseer de procedures voor de uitgifte, wijziging en intrekking van autorisaties van alle autorisaties met betrekking tot Burgernet en leg deze procedures schriftelijk vast. Controleer daarnaast jaarlijks tijdens de interne audit steekproefsgewijs of de afspraken ten aanzien van in-, door- en uitstroom worden nageleefd.

10. **Conclusie**: doordat niet duidelijk de rol of hoedanigheid is benoemd op grond waarvan gemeente ambtenaren toegang hebben tot adresgegevens van deelnemers bestaat het risico dat een rechtsgrond hiervoor ontbreekt.
    Aanbeveling: leg formeel vast in welke rol of hoedanigheid gemeente ambtenaren toegang hebben tot de adresgegevens van de deelnemers en leg vast op welke formele rechtsgrond zij rechtstreeks toegang krijgen.

11. **Conclusie***:* betrokkenen zijn onvoldoende accuraat in het actualiseren van hun eigen gegevens, waardoor op de lange termijn de gegevens steeds minder up-to-date zijn.
    Aanbeveling: bericht deelnemers jaarlijks met een verzoek de juistheid van hun gegevens te controleren.

12. **Conclusie**: omdat afspraken over de beveiliging onvoldoende concreet zijn, bestaat het risico dat daarmee onduidelijkheid ontstaat over de na te leven norm en daarmee persoonsgegevens onvoldoende beveiligd zijn.
    Aanbeveling: onderwerp de huidige afspraken over beveiliging aan een nadere beschouwing en indien de uitkomsten daartoe aanleiding geven, bespreek deze met de verwerker(s).

Bijlage 1 Geïnterviewde personen

1. - programmamanager Burgernet
2. - beleidsadviseur Burgernet
3. - technisch projectleider Burgernet en landelijk functioneel beheerder
4. - landelijk functioneel beheerder

Bijlage 2 Beoordeelde documenten

1. Dossier Afspraken en Procedures 05-11-2019
2. Handleiding Richtlijn Burgernet inzet tijdkritische situaties Burgernet 10-10-2016 versie 3.2
3. Handleiding Digitaal Buurtonderzoek Burgernet 2.0 22-11-2018
4. Handleiding Relatiebeheer Burgernet 2.0 20-11-2018
5. Handleiding Burgernet Informatief/Preventief bericht 2.0 22-11-2018
6. Handleiding Burgernet Vernieuwing Client 2.0 27-05-2019
7. Presentatie Burgernet KMAR 19-09-2019
8. Infobulletin Raadsleden Burgernet 2018
9. Notitie Gemeentelijke taken Burgernet 15-05-2014
10. Verwerkersovereenkomst CGI - Politie 30-08-2018
11. Verwerkersovereenkomst Intermax - Politie 03-09-2018
12. Verwerkersovereenkomst M2MOBI - Politie 17-09-2018
13. Programma Initiatie document Landelijke uitrol Burgernet 25-06-2007
14. Beschrijving Burgernet taken Gemeenten en Politie ongedateerd
15. Brief voorzitter Stuurgroep Burgernet aan eenheidschefs Politie over rollen Burgernet binnen de eenheden 15-06-2105
16. Memo borging politietaken binnen Burgernet 31-08-2017
17. Memo taken Burgernet ongedateerd

Bijlage 3 Overzicht persoonsgegevens op basis van aanbevelingen

Verwerking	Gegevens	Bron	Gegevens afkomstig van	Doel	Verantwoordelijke
Deelnemers-portaal Via website	Adresgegevens Mobiel telefoon-nummer Vast telefoon-nummer E-mailadres	Deelnemer-portaal	Deelnemers	Versturen van alerts Digitaal buurtonderzoeken, Nieuwsberichten, Informatieve berichten	Politie
Burgernet actiebericht	E-mailadres	Burgernet-server	Deelnemer via Deelnemer-portaal bij aanmelding	Opsporing in het kader van artikel 3 Politiewet	Politie
Burgernet actiebericht via sms of spraak	Mobiel telefoon-nummer	Burgernet-server	Deelnemer via Deelnemer-portaal bij aanmelding	Opsporing in het kader van artikel 3 Politiewet	Politie
Burgernet-actiebericht via Burgernet-app	Token (wordt gewist na verzenden pushbericht) Respons	Burgernet app server	Burgernet-app-gebruiker	Opsporing in het kader van artikel 3 Politiewet	Politie
Digitaal buurtonder-zoek via e-mail	E-mailadres Postcode en huisnummer Respons gegevens	Burgernet-server of Burgernet app server	Deelnemer via Deelnemer-portaal bij aanmelding Deelnemer via e-mail op respons digitaal buurtonderzoek	Ontvangen berichten Digitaal buurtonderzoek) in kader van opsporing artikel 3 Politiewet	Politie
Nieuwsbrief, informatief bericht via e-mail	E-mailadres	Burgernet-server	Deelnemer via Deelnemer-portaal bij aanmelding	Ontvangen nieuwsbrieven met algemene informatie over een veilige leefomgeving gericht op preventie in het kader van artikel 172 Gemeentewet	Politie
Facebook messenger	Facebook naam	Facebook	Facebook gebruiker die zich als vriend	Opsporing in het kader van artikel 3 Politiewet	Politie

			heeft aangemeld bij Burgernet		
Twitter	Twitter naam	Twitter	Twitter-gebruiker die het Burgernet-account volgt	Opsporing in het kader van artikel 3 Politiewet	Politie
Dashbord	Statistische gegevens	Google Firebase Burgernet database	Deelnemers, Burgernet-app-gebruikers	Inzicht hoe Burgernet functioneert in een gemeente. Aantal deelnemers per gemeente Trends in het aantal aanmeldingen of downloads van de app. Aantal en de aard van Burgernetacties	Politie
Beheer-portaal	Naam Functie E-mailadres	Beheer-portaal	Beheerders	Beheer van gegevens van deelnemers via de website[27]	Politie

[27] Dit staat niet in de weg aan de reeds bestaande verdeling van taken tussen de Politie en gemeenten over het beheer.

Bijlage 4 Overzicht Burgernetsysteem