Gegevensuitwisseling in het kader van agressie(preventie)

Inhoud: Richtlijnen ten behoeve van het uitwisselen van (persoons)gegevens Binnen de gemeente en tussen de gemeente en samenwerkingspartners, naar aanleiding van agressie-incidenten

Versie: maart 2019

Inleiding

Binnen de gemeentelijke organisatie hebben verschillende afdelingen te maken met dezelfde burgers. In relatie tot veilig werken is de uitwisseling van gegevens over agressie-incidenten tussen afdelingen van belang. Enerzijds om voorafgaand aan het contact met de burger geïnformeerd te zijn over het eventuele risico op agressie en geweld, zodat de juiste voorzorgsmaatregelen getroffen kunnen worden. Anderzijds ook om patronen in het gedrag van een burger te kunnen signaleren en de hierbij behorende aanpak te kiezen, waar nodig vergezeld van sancties.

In het sociaal domein, hebben gemeenten daarnaast diverse samenwerkingsvormen ingericht met ketenpartners. Om goede zorg te kunnen verlenen en de juiste interventies uit te zetten, kan het voor ketenpartners nodig zijn om onderling informatie te delen. Ook voor ketenpartners is de uitwisseling van gegevens van agressie-incidenten van belang om veilig te kunnen werken.

Gemeenten werken met het Gemeentelijk Incidenten Registratiesysteem (GIR) voor het registreren van agressie-incidenten. Binnen het GIR is er de mogelijkheid om gegevens van eerdere agressie-incidenten, gekoppeld aan persoonsgegevens van de veroorzakers te raadplegen.

Gegevensuitwisseling

Er bestaan in de praktijk veel vragen over het al dan niet mogen uitwisselen van dergelijke veroorzakergegevens. Rekening houden met de privacy van burgers is een groot goed en leidt in de praktijk tot een zeer terughoudende reactie binnen gemeenten en tussen gemeenten en ketenpartners als het gaat over het uitwisselen van persoonsgegevens in relatie tot agressie(preventie).
In dit document werken we daarom de spelregels uit ten aanzien van het mogen delen van persoonsgegevens gekoppeld aan agressie-incidenten.

Wettelijk kader

In een samenwerkingsverband tussen een gemeente en ketenpartners, zijn in alle gevallen de volgende wetten van toepassing:

- de Wet basisregistratie personen (Wet BRP); en
- de Algemene Verordening Gegevensbescherming (AVG) en onder omstandigheden ook
- de Richtlijn EU 2016/680.

Doelbinding

De AVG hanteert het doelbindingsbeginsel, wat inhoudt dat persoonsgegevens alleen mogen worden verwerkt voor duidelijk omschreven en gerechtvaardigde doeleinden (artikel 5 AVG). Het doel van de gegevensverzameling bepaalt de hoeveelheid en de soort informatie die gedeeld mag worden.

Over het gemeenschappelijke doel dient men het binnen de gemeente en met ketenpartners eens te zijn, alvorens de, bij het doel passende, informatie mag worden gedeeld.
In deze context is het doel de veiligheid van de medewerkers zoveel mogelijk te waarborgen.

Passend bij dit doel worden in het GIR persoonsgegevens in de vorm van naam en geboortedatum genoteerd, die door onderdelen van de gemeentelijke organisatie en ketenpartners te raadplegen zijn op het moment dat een agressie-incident heeft plaatsgevonden dat is gemeld en waarvoor de gemeente of een ketenpartner een maatregel of sanctie heeft opgelegd.

Het mogen raadplegen van de betreffende gegevens is voorbehouden aan degenen die deze informatie nodig hebben om de veiligheid van medewerkers in het contact met burgers te borgen.

De AVG hanteert ook het evenredigheidsbeginsel. De functie van het verwerken van persoonsgegevens moet in verhouding staan tot de consequenties die dat kan hebben voor de grondrechten van de mens. In de AVG wordt daarbij benoemd dat voor taken van algemeen belang en/of voor de uitvoering van het openbaar gezag, per land in de EU afzonderlijke afspraken kunnen worden gemaakt. Er wordt in de AVG in deze context ook verwezen naar de EU-richtlijn 2016/680. Artikel 5.1 benoemt (onder andere) het uitgangspunt dat persoonsgegevens rechtmatig en eerlijk worden verwerkt, voor welbepaalde, uitdrukkelijk omschreven en legitieme doeleinden. Daarbij wordt benoemd dat de gegevens die worden verwerkt ter zake dienend en niet bovenmatig mogen zijn in de relatie tot de doelen waarvoor ze worden verwerkt.

Verplichtingen ten opzichte van de betrokkenen

Het is niet nodig aan de betrokken burger toestemming te vragen voor het delen van de informatie. Ook in de richtlijn EU 2016/680 is in artikel 13.3 omschreven dat het informeren van betrokkenen over het verwerken van persoonsgegevens achterwege mag blijven als dat een noodzakelijke en evenredige maatregel is ter bescherming van de openbare veiligheid.

Wel stelt de AVG de volgende verplichtingen:

Informatieplicht

De betrokkene dient geïnformeerd te worden over een aantal aspecten van de verwerking, zoals het doel van het vastleggen van zijn/haar persoonsgegevens, de contactgegevens van de verwerkingsverantwoordelijke, de contactgegevens van de functionaris voor de gegevensbescherming (FG), de bewaartermijn, de categorieën van verwerkte gegevens en de rechten van de betrokkene (artikel 12 lid 1 AVG). Ook als informatie gedeeld wordt met ketenpartners moet de betrokkene daarover worden geïnformeerd. In de praktijk nemen gemeenten in sanctie- of maatregelbrieven een zinsnede op waarmee de burger geïnformeerd wordt over het geregistreerde incident en het delen van de informatie.

Betrokkene de mogelijkheid geven zijn/haar rechten uit te oefenen

Een burger wiens persoonsgegevens worden vastgelegd heeft de volgende rechten:

- Recht op inzage (artikel 15 AVG): in het geval dat een burger vraagt om inzage, moet deze worden geïnformeerd over welke gegevens, het doel van de verwerking, eventuele bewaartermijnen, de klachtmogelijkheid bij de toezichthouder in Nederland (Autoriteit Persoonsgegevens) en met wie deze gegevens zijn gedeeld.
- Recht op rectificatie (artikel 16 AVG): in het geval dat de persoonsgegevens onjuist zijn, mag de burger verzoeken om onverwijlde correctie.
- Recht op vergetelheid (artikel 17 AVG): in het geval dat (a) de gegevens niet langer nodig zijn voor de bepaalde doeleinden, (b) de burger bezwaar maakt tegen de verwerking of (c) de gegevens moeten worden gewist om te voldoen aan een wettelijke verplichting, heeft de burger recht om de gegevens te laten wissen.
- Recht op beperking van de verwerking (artikel 18 AVG): in het geval dat (a) de juistheid van de gegevensverwerking wordt betwist door de burger, (b) de verwerking onrechtmatig is, (c) de burger bezwaar heeft gemaakt tegen de verwerking of (d) in het geval dat de verwerking niet meer nodig is voor de bepaalde doeleinden, maar de burger deze gegevens nog wel nodig heeft, kan de burger verzoeken tot beperking van de verwerking.
- Recht op overdraagbaarheid (artikel 20 AVG): de burger heeft het recht om de persoonsgegevens in een gestructureerde, gangbare en machineleesbare vorm te krijgen en deze gegevens over te dragen aan een andere verwerkingsverantwoordelijke.

- Recht van bezwaar (artikel 21 AVG): een burger kan bezwaar maken tegen het gebruik van de persoonsgegevens. Echter, als de gemeente dwingende en gerechtvaardigde reden heeft om de gegevens te gebruiken die zwaarder weegt dan de belangen van de burger, mag daarmee worden doorgegaan.

Beveiligingsplicht
In artikel 32 AVG staat omschreven dat de persoonsgegevens beveiligd bewaard moeten worden, waarbij rekening moet worden gehouden met passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen. De persoonsgegevens worden in dit geval vastgelegd in het GIR. In de informatiebeveiligingsverklaring, behorende bij het GIR, is vastgelegd welke beveiligingsmaatregelen zijn getroffen.
Als kader voor de beveiligingsverklaring worden gebruikt de AVG, BIG (Baseline Informatiebeveiliging Nederlandse Gemeenten), BIR (Baseline Informatiebeveiliging Rijksdienst) en de SSD (Secure Software Development)-norm van het CIP (Centrum Informatiebeveiliging en Privacybescherming).

Documentatieplicht
Het verwerken van persoonsgegevens moet worden bijgehouden in een register (artikel 30 AVG). Er wordt vanuit het GIR geen koppeling gemaakt naar eventuele andere systemen of databestanden. De persoonsgegevens naam en geboortedatum worden geregistreerd om de juiste identificatie van de bij een agressie-incident betrokken burger te kunnen waarborgen en daarmee de medewerkers in staat te stellen, zoveel als mogelijk, te zorgen voor de eigen veiligheid.

<u>Praktisch aan de slag</u>
Als een gemeente, evt. samen met haar ketenpartners in het sociaal domein, binnen beschreven context en kader persoonsgegevens van veroorzakers wil registreren en delen, dan vraagt dat om de volgende stappen:
1. Werkafspraken ten aanzien van gegevensuitwisseling vastleggen. Met ketenpartners wordt een (bindend) convenant gesloten. Besteed in het convenant aandacht aan de gegevensstromen, het doel van de gegevensuitwisseling, de verdeling van aansprakelijkheid, de vertrouwelijkheid van gegevens en dergelijke.
2. Op basis van de afspraken het GIR inrichten, zodat de juiste medewerkers de autorisatie van ‘raadpleger’ krijgen in het systeem. Met deze autorisatie kan door het raadplegen van veroorzakergegevens (naam en geboortedatum) inzicht worden verkregen in een eventuele historie met agressie-incidenten. Alle agressie-incidenten waarbij de veroorzaker betrokken was en die bekend zijn in de betreffende gemeentelijke organisatie en in het sociaal domein, worden getoond. Op basis van deze informatie kunnen de juiste maatregelen worden getroffen in relatie tot de condities waaronder wel/niet dienstverlening wordt geleverd. Als de veroorzakergegevens worden geraadpleegd na een agressie-incident, fungeert het verkregen inzicht in de agressiehistorie als input voor het opleggen van maatregelen of sancties.

Het werken met een zwarte lijst
Vaak gehoord is de vraag naar de mogelijkheid om te werken met een zwarte lijst van veroorzakers van agressie.

Om een zwarte lijst te mogen aanleggen moet er voldaan zijn aan een aantal voorwaarden:
1. Gerechtvaardigd belang
   Er moet sprake zijn van een gerechtvaardigd belang. Normoverschrijdend gedrag bestrijden en zorg dragen voor de veiligheid van medewerkers, zijn voorbeelden van een gerechtvaardigd belang.
2. Noodzaak verwerking persoonsgegevens
   Een zwarte lijst mag alleen gemaakt worden als er geen andere manier is om het doel van de organisatie te bereiken. De privacy van burgers mag niet onnodig in het geding zijn.

3. Afweging belangen
   De gemeente moet duidelijk kunnen maken dat het geplaatst worden op een zwarte lijst (belang van de organisatie) zwaarder weegt dan het privacybelang. Normoverschrijdend gedrag van burgers, waardoor de veiligheid van medewerkers in het geding is en de uitvoering van de taak van de organisatie onder druk staat, is een voorbeeld van een zwaarder wegend belang.

Omdat de Autoriteit Persoonsgegevens een zwarte lijst heeft gekwalificeerd als een verwerking van persoonsgegevens die waarschijnlijk een hoog privacy risico oplevert, is het belangrijk dat de gemeente als verwerkersverantwoordelijke een Data Protection Impact Analyse (DPIA) uitvoert, waarin wordt vastgelegd welke privacyrisico's betaan en hoe deze risico's verkleind worden (door bv. goed na te denken over wie er inzage heeft in de gegevens en vanuit welk doel (gerechtvaardigd belang).

Meer informatie over de DPIA is te vinden op:
1. DPIA voorlichting van de Autoriteit Persoonsgegevens
2. DPIA checklist voor nieuwe verwerkingen.
3. Daarnaast heeft de VNG een checklist uitgebracht voor de DPIA. Wij hebben deze niet gecheckt.

Verwijzingen:
- Informatie delen in samenwerkingsverbanden; Autoriteit Persoonsgegevens
- Richtlijn EU2016/680
- Verordening (EU) 2016/679 van het Europees parlement en de Raad; 27 april 2016: betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming)
- Verwerkersovereenkomst Gemeentelijk Incidenten Registratiesysteem (GIR)