RAADSINFORMATIEBRIEF
19R.00164

Van : college van burgemeester en wethouders
Datum : 9 april 2019
Portefeuillehouder(s) : Burgemeester
Portefeuille(s) : Openbare Orde en Veiligheid
Contactpersoon : T. Vermeulen
Tel.nr. : 8292
E-mailadres : vermeulen.t@woerden.nl

Onderwerp:

Cameratoezicht winkelcentrum Tournoysveld

Kennisnemen van:

De burgemeester heeft beoordeeld of het inzetten van cameratoezicht bij het winkelcentrum Tournoysveld voldoet aan de eisen van proportionaliteit en subsidiariteit, waarover u in deze RIB meer leest. Daarnaast is een Privacy Impact Assessment (PIA) uitgevoerd naar aanleiding van de motie van de gemeenteraad om te onderzoeken of cameratoezicht kan worden ingesteld.

Inleiding:

In de gemeenteraadsvergadering d.d. 22 februari 2019 heeft de gemeenteraad een motie aangenomen waarin wordt gevraagd een brede aanpak van de problematiek rondom het winkelcentrum Tournoysveld te onderzoeken. De burgemeester heeft in een eerder stadium tijdens een bijeenkomst van het wijkplatform reeds toegezegd de mogelijkheid tot het instellen van cameratoezicht te willen onderzoeken. Naar aanleiding van deze ontwikkeling heeft de afdeling OOV in samenwerking met de Functionaris Gegevensbescherming een PIA uitgevoerd, om te beoordelen welke gevolgen het verwerken van persoonsgegevens bij cameratoezicht heeft op de privacy van betrokkenen.

Kernboodschap:

<u>Proportionaliteit</u>
Al sinds enige maanden zijn er incidenten bij het winkelcentrum die bij de gemeente en politie bekend zijn. Deze meldingen hebben onder andere betrekking op overlast door rondhangende jeugd, maar ook meer serieuze incidenten als autobranden, vandalisme tegen auto's en agressie tegen winkeleigenaren. Zo is enkele maanden geleden een stoeptegel door de ruit van een horecagelegenheid gegooid. Met name de autobranden rondom het winkelcentrum hebben tot veel maatschappelijke onrust geleid. In totaliteit vormen deze incidenten een risico op een ernstige verstoring van de openbare orde, waarbij het meermaals is voorgekomen dat zich daadwerkelijke verstoringen van de openbare orde hebben voorgedaan. Ook het feit dat deze incidenten zich verspreid over meerdere maanden hebben voorgedaan laat zien dat de verstoringen van de openbare orde van structurele aard zijn. De ernst en langdurigheid van de incidenten maakt dat de gegevensverwerking als gevolg van de inzet van cameratoezicht naar inzicht van de burgemeester proportioneel is.

<u>Subsidiariteit</u>
Naar aanleiding van bovengeschetste incidenten heeft de gemeente eerder maatregelen getroffen. Zo is de politie in de buurt extra gaan surveilleren, hebben BOA's extra aandacht aan het winkelcentrum besteed en hebben jongerenwerkers gericht de groep overlastgevende jongeren benaderd. Dit heeft echter nauwelijks geleid tot een afname van de ervaren overlast en daadwerkelijke incidenten. Na het treffen van deze

maatregelen hebben zich zelfs nog twee autobranden voorgedaan. Daarmee zijn eerder maatregelen getroffen die niet toereikend zijn gebleken om de problematiek op te lossen en welke ook niet in redelijkheid kunnen worden uitgebreid. Als de surveillances nog meer zouden worden uitgebreid zou dit teveel capaciteit van politie, BOA's en jongerenwerkers vragen waardoor andere delen van de gemeente niet meer op het gewenste niveau bediend kunnen worden. Deze situatie rechtvaardigt dat de gegevensverwerking als gevolg van cameratoezicht wordt ingezet waarbij een beperkte inbreuk wordt gemaakt op de belangen van betrokkenen.

In reactie op de meest recente ontwikkelingen heeft de gemeente een aanvullend plan van aanpak gemaakt, waar het instellen van cameratoezicht een onderdeel van uitmaakt. Hierin wordt een aantal maatregelen geschetst die reeds zijn getroffen of in uitvoering zijn. Concreet behelst dit:

- Instellen camerabewaking door eigenaar van het winkelcentrum
- Het gezamenlijk opstarten van een traject voor Keurmerk Veilig Ondernemen (KVO)
- In beeld brengen van overlastgevende personen
- Bekende criminelen/overlastgevenden in een PGA-traject plaatsen
- Verlichting rondom het winkelcentrum beter op orde brengen
- Prullenbakken plaatsen
- Uitvoeren van aanvullend groenonderhoud om beter zicht te krijgen op beschutte plekken
- Contact opnemen met andere gemeenten om ervaringen/inzichten te verkrijgen
- Instellen van cameratoezicht voor het handhaven van de openbare orde

<u>Privacy Impact Assessment</u>
Sinds de invoering van de AVG is de burgemeester verplicht een Privacy Impact Assessment te maken alvorens cameratoezicht wordt ingezet. De afdeling OOV en de Functionaris Gegevensbescherming hebben gezamenlijk deze PIA uitgevoerd en hebben geïnventariseerd welke gevolgen het verwerken van persoonsgegevens door cameratoezicht heeft op de privacy van betrokkenen. De PIA vindt u bijgevoegd.

De PIA is een zeer algemeen instrument, dat voor alle soorten gegevensverwerking kan worden gebruikt. Er zitten veel controlevragen in waaruit kan voortvloeien dat aanvullende waarborgen ten aanzien van de privacy worden geadviseerd. Het instrument cameratoezicht is echter een middel dat reeds omkleed is met zeer specifieke en strenge wetgeving ten aanzien van privacy. Veel van de adviezen die uit de PIA naar voren komen zijn reeds ondervangen. Ook het feit dat camerabeelden pas worden uitgelezen op het moment dat zich een incident voordoet, betekent een veel minder grote impact dan wanneer live uitgekeken zou worden. Deze nuance wordt in de PIA echter niet onderkend.

Er worden naar aanleiding van de PIA twee concrete aanvullende acties ondernomen die nog niet zijn ingebed:

- Er wordt een verwerkersovereenkomst gesloten met de leverancier van de camerasystemen;
- Er worden afspraken gemaakt over de wijze van vernietiging van de camerabeelden achteraf zodat deze in lijn is met de gemeentelijke standaard.

Financiën:

In de tussentijd is bij verschillende leveranciers een vrijblijvende offerte opgevraagd om cameratoezicht in te stellen. De aanbieding die de voorkeur verdient levert 4 stand-alone camerasystemen met 360-graden zicht, zijn 'hufterproof' en slaan het beeldmateriaal 28 dagen op in overeenstemming met de wettelijke termijnen. De kosten om deze camera's zes maanden in werking te laten staan bedragen ca. €19.000,-. Om het cameratoezicht zo snel mogelijk te installeren zal dit bedrag een overschrijding op het budget van het cluster OOV opleveren.

Vervolg:

Naar aanleiding van de PIA heeft de burgemeester besloten cameratoezicht rondom het winkelcentrum Tournoysveld in te stellen. Het traject hiervoor is inmiddels in gang gezet.

Bijlagen:

1. Privacy Impact Assessment cameratoezicht winkelcentrum Tournoysveld, in corsa geregistreerd onder nummer 19.007022.

De secretaris,

drs. M.H.J. van Kruijsbergen MBA

De burgemeester,

V.J.H. Molkenboer

PIA Rapport

Ingevuld door: Stef Nicolasen op 28-03-2019

Proces: Uitvoering openbare orde en veiligheid

Lijst met bewerkingen:

Cameratoezicht Openbare Orde en Veiligheid Toezicht in kader van Openbare Orde en Veiligheid

	Vraag	Antwoord
1.1	1. Project, proces of de gegevensuitwisseling Is er sprake van het verwerken van persoonsgegevens? Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van Terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.	Ja Op basis van voertuigkentekens kunnen camerabeelden in verband worden gebracht met persoonsgegevens. Advies: Ga verder
1.2	1. Project, proces of de gegevensuitwisseling Is het duidelijk wie verantwoordelijk is voor de verwerking van de gegevens? Bij het beantwoorden dient u rekening te houden met: 1. Voor en door wie het project wordt uitgevoerd? 2. Of er iemand formeel verantwoordelijk is voor de verwerking van de gegevens? 3. Of er een intern contactpersoon is?	Ja De burgemeester bepaalt doel en middelen en is op rond van de AVG verwerkingsverantwoordelijke. Advies: Ga verder naar de volgende vraag
1.3	1. Project, proces of de gegevensuitwisseling Verwerkt je organisatie de persoonsgegevens in opdracht en onder verantwoordelijkheid van een andere organisatie? Ofwel: Treedt je organisatie op als verwerker? Deze vragenlijst is bedoeld voor organisaties die persoonsgegevens verwerken in de rol van verantwoordelijke. Deze vragenlijst is niet bedoeld voor organisaties die persoonsgegevens verwerken in de rol van verwerker.	Nee De gegevens blijven onder beheer van de gemeente tot vernietiging na 4 weken. Incidenteel worden de data ter beschikking gesteld van de politie (op basis van incidenten). Advies: Bepaal wie (bedrijfsonderdeel, persoon) binnen de organisatie verantwoordelijke is.

	Vraag	Antwoord
1.4	1. Project, proces of de gegevensuitwisseling Is het duidelijk wie na afloop van het project, proces of gegevensuitwisseling verantwoordelijk is voor het in stand houden en evalueren van de getroffen maatregelen? Uiteraard moeten ook in de toekomst de getroffen maatregelen in stand gehouden worden en worden gezorgd dat de risico’s worden beheerst (bijvoorbeeld door deze PIA periodiek uit te voeren)	Ja De burgemeester. Advies: Ga verder met de volgende vraag
1.5	1. Project, proces of de gegevensuitwisseling Is het doel van de verwerking van persoonsgegevens voldoende SMART omschreven? SMART staat voor: Specifiek: de doelstelling moet eenduidig zijn Meetbaar: onder welke (meetbare/observeerbare) voorwaarden of vorm is het doel bereikt. Acceptabel: is deze acceptabel genoeg voor de doelgroep en/of management. Realistisch: is de doelstelling haalbaar. Tijdgebonden: wanneer het doel afgerond moet zijn.	Ja Primair preventief in kader van handhaving openbare orde en niet de opsporing van strafbare feiten. Betreft tijdelijke maatregel (6 maanden met mogelijkheid tot verlenging). Advies: Ga verder met de volgende vraag
1.6	1. Project, proces of de gegevensuitwisseling Is er sprake van gebruik van nieuwe technologie? Bijvoorbeeld intelligente transportsystemen, locatie of volgsystemen op basis van GPS, mobiele technologie, gezichtsherkenning in samenhang met cameratoezicht.	Nee Geen gezichtsherkenning. Advies: Ga verder met de volgende vraag
1.6.1	1. Project, proces of de gegevensuitwisseling Is er sprake van gebruik van technologie die bij het publiek vragen of weerstand op kan roepen? Bijvoorbeeld biometrie, RFID, behavioural targeting (profilering).	Nee Er kan enige vorm van profilering optreden naar aanleiding van strafbare feiten.Dat valt vervolgens onder de Wet Politiegegevens. Advies: Ga verder met de volgende vraag

	Vraag	Antwoord
1.6.2	1. Project, proces of de gegevensuitwisseling Is er sprake van de invoering van bestaande technologie in een nieuwe context? Zoals cameratoezicht of drugscontrole op de werkvloer.	Nee Cameratoezicht in de openbare ruimte is reeds tweemaal eerder toegepast in Woerden. In kader van handhaving OOV is de acceptatie groot. Advies: Ga verder met de volgende vraag
1.6.3	1. Project, proces of de gegevensuitwisseling Is er sprake van andere grote verschuivingen in de werkwijze van de organisatie, de manier waarop persoonsgegevens worden verwerkt en/of de technologie die daarbij gebruikt wordt? Bijvoorbeeld het samenvoegen koppelen van verschillende overheidsregistraties, invoering van nieuwe vormen van identificatie of vervanging van systeem waarin persoonsgegevens worden opgeslagen?	Nee AFzonderlijke opslag van de gegenereerde data. Advies: Ga verder met de volgende vraag
1.6.4	1. Project, proces of de gegevensuitwisseling Is er sprake van een nieuwe verwerking van persoonsgegevens? a. Het gebruik van gegevens voor andere bedrijfsprocessen dan waarvoor ze zijn verzameld, of bredere verspreiding van de gegevens binnen of buiten de organisatie. b. Bij een eerste beoordeling ook PIA doorlopen wanneer er nog geen PIA is uitgevoerd in het verleden.	Ja Advies: Uw risicoprofiel verandert. Er wordt geadviseerd een compliance check uit te voeren. Dergelijke projecten vragen om een goede beoordeling van de consequenties op het gebied van privacy.
1.6.5	1.Project, proces of de gegevensuitwisseling Is er sprake van het verzamelen van meer of andere persoonsgegevens dan voorheen of een nieuwe manier van verzamelen? Bijvoorbeeld gegevensverrijking door enquêtes en klantonderzoek of benadering van klanten/burgers op basis van beschikbare gegevens voor nieuwe producten of diensten.	Ja Advies: Uw risicoprofiel verandert. Er wordt geadviseerd een compliance check uit te voeren. Dergelijke projecten vragen om een goede beoordeling van de consequenties op het gebied van privacy.

	Vraag	Antwoord
1.6.6	1. Project, proces of de gegevensuitwisseling Is er sprake van gebruik van al verzamelde gegevens voor een nieuw doel of een nieuwe manier van gebruiken? Bijvoorbeeld het samenvoegen van interne databases om klantprofielen op te stellen.	Nee Advies: Ga verder met de volgende vraag
1.7	1. Project, proces of de gegevensuitwisseling Heeft u op alle bovenstaande vragen t/m 1.6.6 "nee" geantwoord?	Nee Advies: Ga verder met de volgende vraag
1.8	1. Project, proces of de gegevensuitwisseling Is er (naast de Wbp/GDPR) wet en regelgeving ten aanzien van persoonsgegevens waar het project, proces of gegevensuitwisseling mee te maken heeft? Denk aan: 1. Sectorale wetgeving. 2. Gedragscodes. 3. Algemene maatregelen van bestuur. 4. Jurisprudentie. 5. Internationale aspecten. 6. Afspraken in samenwerkindsverbanden, zoals modelovereenkomsten e.z.v.	Ja Wet Politiegegevens Advies: U loopt een verhoogd risico. Hoe meer wet- en regelgeving des te hoger het risico dat u hieraan niet voldoet. Een grote hoeveelheid wet- en regelgeving duidt tevens op het maatschappelijk belang dat wordt gehecht aan het onderwerp. U wordt geadviseerd de van toepassing zijnde wet- en regelgeving in kaart te brengen en de (privacy) consequenties inzichtelijk te maken.
1.9	1. Project, proces of de gegevensuitwisseling Zijn er veel maatschappelijke belanghebbenden? Denk aan: 1. Medewerkers, afnemers, leveranciers, belangengroeperingen, burgers, klanten toezichthouders. 2. Stichtingen, verenigingen, zoals personeelsvereniging. 3. OR. 4. Vrijwilligers.	Nee Betreft Openbare Orde en veiligheid: in die zin maatschappij als geheel baat hebbend. Advies: Ga verder met de volgende vraag

	Vraag	Antwoord
1.10	1. Project, proces of de gegevensuitwisseling Zijn er veel partijen betrokken bij de uitvoering van het project, proces of gegevensuitwisseling? Houd bij de beantwoording rekening met: 1. Aannemers en dienstverleners. 2. Hard en software leveranciers. 3. IT service privider 4. Cloud services. 5. App-store programeurs, dienstverleners, leveranciers 6. Internet of Things leveranciers, dienstverleners	Nee Advies: Ga verder met de volgende vraag
1.11	1. Project, proces of de gegevensuitwisseling Is er een geschillenregeling/partij waar betrokkene terecht kan bij vragen of klachten? Op instellingsniveau (als verwerker) of als lid van een brancheorganisatie of met behulp van AP.	Ja De FG van de gemeente Woerden. Advies: Ga verder met de volgende vraag
2.1	2. De gegevens Zijn alle gegevens nodig om het doel te bereiken (worden er zo min mogelijk gegevens verzameld)? U dient bij de beantwoording rekening te houden met: - Is per data-element vastgesteld wat de toegevoegde waarde is en waarom dit noodzakelijk is? - Kan volstaan worden met het gebruik van alleen ja/nee in plaats van het volledige gegeven? - Kan volstaan worden met het verschil tussen 2 waarden in plaats van beide waarden afzonderlijk? - Kan gebruikgemaakt worden van andere wiskundige methodieken (bijvoorbeeld voor het bepalen van afwijkingen)?	Ja Beelden worden alleen uitgelezen na incidenten. Advies: Ga verder met de volgende vraag

	Vraag	Antwoord
2.2	2. De gegevens Kan het doel met geanonimiseerde of gepseudonimiseerde gegevens worden bereikt (terwijl daar op dit moment geen gebruik van wordt gemaakt)? Door pseudonimisering, worden de direct identificerende gegevens van de betrokkene op een eenduidige wijze vervangen waardoor in de toekomst bepaalde partijen nog steeds gegevens kunnen toevoegen. Door anonimisering worden alle direct, uniek identificerende gegevens verwijderd.	Nee Gegevens zijn anoniem, kunnen slechts worden gekoppeld aan bijv. kentekenregistratie. Advies: Ga verder met de volgende vraag
2.3	2. De gegevens Kunnen de gegevens gebruikt worden om het gedrag, de aanwezigheid of prestaties van mensen in kaart te brengen en/of te beoordelen (ook al is dit niet het doel)? Denk hierbij bijvoorbeeld ook aan geolocatie, personeelsvolgsystemen, beslisondersteuning bij het als dan niet aanbieden van producten of diensten.	Ja Advies: U loopt een verhoogd risico. Het risico bestaat dat de betrokkenen of de algemene opinie dit als een potentiële bedreiging voor hun privacy zien. Ook als de gegevens niet voor dit doel worden gebruikt, bestaat het risico dat dit (in de toekomst) wel gebeurd.
2.4	2. De gegevens Is er sprake van bijzondere persoonsgegevens? De Wbp (artikel 16) en GDPR (artikel 9) noemt zogenaamde bijzondere persoonsgegevens: persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, persoonsgegevens betreffende het lidmaatschap van een vakvereniging, strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.	Ja Etniciteit. Advies: Het werken met dit type gegevens brengt een verhoogd risico van misbruik met zich mee die (potentieel grote) impact heeft op de betrokkene en vraagt daarmee om betere beveiliging. Het verwerken van deze gegevens is alleen toegestaan onder bepaalde wettelijke voorwaarden (art. 16 Wbp / art. 9 GDPR).

	Vraag	Antwoord
2.4.1	2. De gegevens Is er sprake van uniek identificerende gegevens? Bijvoorbeeld biometrische gegevens, vingerafdrukken, DNA-profielen. Het unieke patiëntennummer van de zorginstelling.	Nee Advies: Ga verder met de volgende vraag
2.4.2	2. De gegevens Is er sprake van wettelijk voorgeschreven persoonsnummers? Bijvoorbeeld het burgerservicenummer (BSN)	Nee Advies: Ga verder met de volgende vraag
2.4.3	2. De gegevens Is er sprake van andere gegevens dan hiervoor beschreven waarvoor geldt dat sprake is van een (gepercipieerde) verhoogde gevoeligheid? Bijvoorbeeld creditcardinformatie, financiële informatie, erfrechtelijke aspecten, arbeidsprestaties of gegevens waarvoor een geheimhoudingsplicht geldt.	Nee Advies: Ga verder met de volgende vraag
2.4.4	2. De gegevens Indien één van de vragen (2.4 -2.4.3) met "Ja" is beantwoord: Kan het doel met andere gegevens worden bereikt die een verminderd risico op misbruik met zich mee brengen?	Nee Advies: Ga verder met de volgende vraag

	Vraag	Antwoord
2.5	2. De gegevens Verwerkt u gegevens over kwetsbare groepen of personen? Bijvoorbeeld minderjarige personen, verstandelijk gehandicapten, gedetineerden, onder toezicht gestelden, mensen van wie de fysieke veiligheid in gevaar is.	Ja Situationeel afhankelijk. Advies: U loopt een verhoogd risico. Indien deze gegevens worden misbruikt heeft dit negatieve beeldvorming in de publieke opinie over de organisatie tot gevolg. U wordt geadviseerd maatregelen te treffen op een hoger beveiligingsniveau (art. 13 Wbp / art. 28 GDPR) en betrokkenen de mogelijkheid te bieden zich aan de verwerking te onttrekken.
2.6	2. De gegevens Betreft het een verwerking van persoonsgegevens met meer dan 5000 betrokkenen op jaarbasis?	Ja Advies: U loopt een verhoogd risico. De kans op misbruik van de gegevens wordt groter naarmate u meer gegevens verwerkt. U wordt geadviseerd maatregelen te treffen op een hoger beveiligingsniveau (art. 13 Wbp / art. 28 GDPR).
3.1	3. Betrokken partijen Zijn er (na afronding van het project, proces of gegevensuitwisseling) bij het verzamelen en verder verwerken van de gegevens meerdere interne partijen betrokken? Denk aan: 1. Afdelingen die gebruikmaken van de gegevens. 2. Afdelingen die de gegevens verzamelen. 3. De personen die toegang hebben tot de gegevens.	Nee Advies: Ga verder met de volgende vraag

	Vraag	Antwoord
3.2	3. Betrokken partijen Zijn er (na afronding van het project, proces of gegevensuitwisseling) bij het verzamelen en verder verwerken van de gegevens meerdere externe partijen betrokken? Denk aan: 1. Voor en door wie het project wordt uitgevoerd. 2. Welke partijen gebruikmaken van de gegevens. 3. Of andere partijen worden ingeschakeld voor het bereiken van het doel (wordt de verwerking van gegevens ge-outsourced). 4. Of de gegevens worden verkocht. 5. Welke personen buiten de organisatie toegang hebben tot de gegevens. 6. Wie is de eigenaar van de gegevens. 7. Wie zijn de subverwerkers.	Ja Alleen eventueel de politie en leverancier camera's. Advies: U loopt een verhoogd risico. Hoe meer partijen betrokken zijn, hoe groter de kans op verlies van gegevens, onduidelijkheden in verantwoordelijkheden, het gebruik van de gegevens voor andere doelen en de kans op fouten. Zorg voor een duidelijke beschrijving van taken en verantwoordelijkheden met betrekking tot de gegevens waarbij onder andere wordt beschreven: - Beveiliging van gegevens; - Afhandeling van fouten; - Terugmelden van fouten; - Afstemming van het beveiligingsbeleid; - Controle. Zorg voor een duidelijke gegevensbeschrijving. Leg afspraken contractueel vast.
3.3	3. Betrokken partijen Zijn er partijen betrokken (in het project, proces of gegevensuitwisseling of bij de verwerking) die zich niet aan een met Nederland vergelijkbare privacywetgeving hoeven te houden? Voor gegevens die worden verwerkt buiten de Europese Economische Ruimte (EER) moet een adequaat niveau van bescherming geboden worden. Alle landen binnen de EER dienen te voldoen aan de Europese gegevensbeschermingsrichtlijn. De Europese Commissie neemt een beslissing over het passend zijn van het geboden beschermingsniveau voor landen buiten de EER. Een lijst van deze landen kan gevonden worden op internet website Autoriteit Persoonsgegevens. Houd bij het beantwoorden van deze vraag rekening met: 1. Of de gegevens van het grondgebied komen waar ze worden opgeslagen. 2. Of de gegevens aan partijen worden verstrekt die niet op het grondgebied zijn gevestigd waar de gegevens worden verzameld.	Nee Advies: Ga verder met de volgende vraag

	Vraag	Antwoord
3.4	3. Betrokken partijen Is de verstrekking van de gegevens aan derde partijen in lijn met het doel waarvoor de gegevens oorspronkelijk zijn verzameld? Denk aan: 1. Wat het doel is voor het gebruik van de gegevens. 2. Welke gegevens aan wie worden verstrekt voor welk doel. 3. De verstrekking aan andere partijen een wettelijke verplichting is. 4. Andere partijen ingeschakeld worden voor het bereiken van het doel (outsourcing). 5. Hoe vaak (frequentie) worden de gegevens aan andere partijen verstrekt (eenmalig, periodieke update, continue). 6. Op welke wijze gegevens worden verstrekt aan andere partijen. 7. Wordt vastgelegd aan welke partijen gegevens worden verstrekt. 8. De andere partij soortgelijke gegevens ontvangt op basis waarvan te herleiden valt op wie de gegevens betrekking hebben (indien deze geanonimiseerd of gepseudonimiseerd zijn). 9. De andere partij soortgelijke gegevens ontvangt op basis waarvan te herleiden valt op wie de gegevens betrekking hebben (indien deze geanonimiseerd of gepseudonimiseerd zijn).	Ja Ingeval van strafbare feiten t.b.v. opsporing en vervolging. Advies: Ga verder met de volgende vraag
3.5	3. Betrokken partijen Worden de gegevens verkocht aan de derde partijen? De Wbp stelt voorwaarden aan het gebruik van gegevens voor commerciële of goede doelen, zoals recht van weigering.	Nee Advies: Ga verder met de volgende vraag
4.1	4. Verzamelen van gegevens Kan de manier waarop de gegevens worden verzameld worden opgevat als privacy gevoelig? Bijvoorbeeld omdat intieme of gevoelige informatie wordt gevraagd in een publiek gebied waar anderen dit kunnen horen, of omdat gebruik gemaakt wordt van (camera)observatie, tracking door cookies of GPS?	Ja Op minder ingrijpende manier het resultaat bereiken is gepoogd, maar levert onvoldoende resultaat. Advies: U wordt geadviseerd na te gaan of de gegevens op een andere manier kunnen worden verzameld.

	Vraag	Antwoord
4.2	4. Verzamelen van gegevens Is het doel van het verzamelen van de gegevens publiekelijk bekend of kan het publiekelijk bekend gemaakt worden? U moet bij de beantwoording rekening houden met of de betrokkene redelijkerwijs op de hoogte kan zijn van de verwerking van de gegevens.	Ja Wordt gewaarschuwd met bordjes. Advies: Ga verder met de volgende vraag
4.3	4. Verzamelen van gegevens Verzamelt u de gegevens op basis van een van de wettelijke grondslagen? De Wbp/GDPR kent een beperkt aantal grondslagen op basis waarvan gegevens mogen worden verwerkt: - Je vraagt toestemming. - De gegevens zijn noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene een partij is. - De gegevens zijn nodig voor het volgen van een wettelijke verplichting. - De betrokkene heeft er een vitaal belang bij dat je de gegevens verzamelt. - De gegevens zijn nodig voor de goede vervulling van een publiekrechtelijke taak. - Je hebt een gerechtvaardigd belang bij de verwerking.	Ja Advies: Ga verder met de volgende vraag
4.4	4. Verzamelen van gegevens Is duidelijk of je de gegevens verzamelt op basis van toestemming (opt-in) of op basis van een andere grondslag(opt-out)? Bij het verwerken van de gegevens moet duidelijk zijn of de betrokkene toestemming moet geven (opt-in) of dat niet hoeft, maar later bezwaar kan maken (opt-out)	Ja Geen toestemming vereist. Advies: Ga verder met de volgende vraag
4.4.1	4. Verzamelen van gegevens Indien je toestemming aan de betrokkene vraagt (opt-in) kunnen de betrokkenen de toestemming op een later tijdstip intrekken (opt-out)? Deze toestemming moet een vrije, specifieke en op informatie berustende wilsuiting zijn.	Ja Advies: Ga verder met de volgende vraag

	Vraag	Antwoord
4.4.2	4. Verzamelen van gegevens Is de impact van het intrekken van de toestemming groot voor de betrokkene? Bijvoorbeeld omdat dienstverlening aan betrokkene stopgezet wordt terwijl deze daarvan afhankelijk is.	Nee Advies: Ga verder met de volgende vraag
4.5	4. Verzamelen van gegevens Vertelt u tegen de betrokkene dat de gegevens worden verzameld? U moet bij de beantwoording rekening houden met: 1. Waar de gegevens vandaan komen (van de betrokkene, een in terne afdeling, een andere partij, uit eigen waarneming, et cetera). 2. Op welke wijze de gegevens worden verzameld. 3. De mogelijkheid dat de betrokkene redelijkerwijs op de hoogte kan zijn van de verwerking van de gegevens. 4. De mate waarin de betrokkene wordt geïnformeerd. 5. De gebruikte technologie. 6. Wat het doel is/ doelen zijn voor het gebruik. 7. Of de gegevens of uitkomsten van gegevensbewerking intern binnen het bedrijf verspreid worden. 8. Op welke wijze (mondeling, schriftelijk, automatisch, elektronisch, waarneming, papier) worden de gegevens aan andere partijen verstrekt. 9. Hoe lang de gegevens worden bewaard. 10. Op welke manier worden de gegevens verwijderd.	Ja Advies: Ga verder met vraag 4.5.2
4.5.2	4. Verzamelen van gegevens Indien op de vraag 4.5 "Ja" is geantwoord: Vertelt u tegen de betrokkene waarom de gegevens worden verzameld (wat u er mee gaat doen)?	Ja Voorlichting team Communicatie. Advies: Ga verder met de volgende vraag
4.5.3	4 Verzamelen van gegevens Indien op de vraag 4.5 "Ja" is geantwoord: Vertelt u tegen de betrokkene aan wie de gegevens worden verstrekt (daar waar dit geen wettelijke verplichting is)?	Ja Wordt in communicatie meegenomen. Advies: Ga verder met de volgende vraag

	Vraag	Antwoord
4.6	4. Verzamelen van gegevens Zou de betrokkene kunnen worden verrast door de verwerking (op het moment dat hij daarover wordt geïnformeerd)? U moet bij beantwoording rekening houden met: 1. De mate waarin de betrokkene wordt geïnformeerd. 2. Hoe gegevens worden verzameld (langs welke weg). 3. De gebruikte technologie. 4. De mogelijkheid dat de betrokkene redelijkerwijs op de hoogte kan zijn van de verwerking van de gegevens. 5. Waar gegevens vandaan komen, van de betrokkene, een interne afdeling, een andere partij, uit eigen waarneming, et cetera. 6. Wat het doel is / doelen zijn voor het gebruik. 7. Of gegevens/uitkomsten van gegevensverwerking intern binnen het bedrijf verspreid worden. 8. Op welke wijze (mondeling, schriftelijk, automatisch, elektronisch, waarneming, papier) worden de gegevens aan andere partijen verstrekt. 9. Hoe lang de gegevens worden bewaard. 10. Op welke manier worden de gegevens verwijderd.	Nee Naast communicatietraject worden er waarschuwingsbordjes opgehangen. Advies: Ga verder met de volgende vraag
5.1	5. Gebruik van gegevens Is het gebruik van de gegevens verenigbaar of in lijn met het doel (grondslag) van het verzamelen? Denk aan: 1. Wat het verzameldoel is. 2. Waarvoor de gegevens worden gebruikt. 3. Welke gegevens worden verzameld. 4. Of deze gegevens bijzondere gegevens betreffen. 5. Waar gegevens vandaan komen, van de betrokkene, een interne afdeling, een andere partij, uit eigen waarneming, et cetera. 6. Hoe vaak (frequentie) de gegevens worden verzameld (eenmalig, regelmatig of voortdurend). 7. Op welke wijze (mondeling, schriftelijk, automatisch, elektronisch, waarneming, papier) de gegevens worden verzameld en verspreid. 8. Welke afdelingen/personen en andere partijen toegang hebben tot de gegevens.	Ja Advies: Ga verder met de volgende vraag

	Vraag	Antwoord
5.2	5. Gebruik van gegevens Worden gegevens gebruikt voor andere bedrijfsprocessen of doelen dan waar ze oorspronkelijk voor verzameld zijn?	Nee Advies: Ga verder naar vraag 5.3
5.3	5. Gebruik van gegevens Is de kwaliteit van de gegevens gewaarborgd, dat wil zeggen: zijn de gegevens actueel, juist en volledig? U moet bij beantwoording rekening houden met: 1. Of gegevens worden gecontroleerd, op welke wijze en op welke aspecten controle plaatsvindt. 2. Of de gegevens kunnen worden gecorrigeerd. 3. Welke personen toegang hebben tot gegevens voor correctie, verwijderen etc. van de gegevens. 4. Welke afdelingen toegang hebben tot de gegevens. 5. Hoe vaak de gegevens worden geüpdate. 6. Wat gevolgen zijn van het gebruiken van onjuiste gegevens. 7. Of maatregelen getroffen wor den om ander gebruik dan het beoogde te voorkomen. 8. Of kwaliteitswaarborgen worden verstrekt bij verstrekking van de gegevens. 9. Wat er gebeurt als (delen van) de gegevens niet aan de andere partijen worden verstrekt.	Ja Advies: Ga verder met de volgende vraag
5.4	5. Gebruik van gegevens Worden op basis van de gegevens beslissingen genomen over de betrokkenen?	Nee Behoudens bij strafbare feiten. Beslissing ligt bij OM. Advies: Ga verder met vraag 5.5
5.5	5. Gebruik van gegevens Is sprake van koppeling, verrijking of vergelijking van gegevens uit verschillende bronnen?	Nee Behoudens bij strafbare feiten indien mogelijk, kentekenregister. Advies: Ga verder met de volgende vraag

	Vraag	Antwoord
5.6	5. Gebruik van gegevens Worden gegevens breed verspreid binnen de organisatie? Denk aan: 1. Welke afdelingen toegang hebben tot de gegevens. 2. Welke personen toegang hebben tot de gegevens. 3. De doelen en het gebruik van de gegevens.	Nee Advies: Ga verder met de volgende vraag
5.7	5. Gebruik van gegevens Worden gegevens breed verspreid buiten de organisatie? Denk aan: 1. Welke organisaties en personen toegang tot de gegevens hebben. 2. Hoe vaak (frequentie) de gegevens worden verstrekt. 3. Het medium dat gebruikt wordt voor verspreiding (bv. papier, CD-ROM) 4. De maatregelen om ander gebruik te voorkomen.	Nee Advies: Ga verder met vraag 5.8
5.8	5. Gebruik van gegevens Stelt uw organisatie profielen op van de betrokkenen, al dan niet geanonimiseerd? Denk hierbij aan profielen op basis van het gebruik van diensten, de afname van producten of bepaalde combinaties van eigenschappen.	Nee Advies: Ga verder met vraag 5.9
5.9	5. Gebruik van gegevens Kunnen de betrokkenen hun gegevens inzien of daarom vragen? Hierbij kan gedacht worden aan reactie op verzoeken of het geven van inzage in eigen gegevens door middel van een informatiesysteem, waarbij wel moet vast staan dat gegevens alleen ingezien kunnen worden door personen die dat mogen.	Nee Gegevens vallen onder de Wet Politiegegevens. Die gegevens vallen onder de geheimhoudingsplicht. Advies: U loopt een verhoogd risico. Betrokkenen hebben het recht hun gegevens in te zien. Hierbij is het van belang dat u zelf ook een helder overzicht heeft van de gegevens die worden verwerkt en waar deze zich binnen de organisatie bevinden. U loopt ook een compliance risico aangezien het verplicht is betrokkenen (op verzoek, eventueel tegen redelijke vergoeding) inzage te geven (art. 35 Wbp / art. 15 GDPR).

	Vraag	Antwoord
5.10	5. Gebruik van gegevens Kunnen de betrokkenen hun gegevens corrigeren of daarom vragen (verbeteren, aanvullen)? Hierbij kan gedacht worden aan het vragen van een reactie op opgestuurde overzichten of het geven van (eigen) correctiemogelijkheden in de eigen gegevens door middel van een informatiesysteem (waarbij de betrokkene wel op een toereikende wijze geïdentificeerd dient te worden).	Nee Realiteit kan niet worden gemuteerd. Advies: U loopt een verhoogd risico. Het bieden van een mogelijkheid tot correctie verbetert de gegevenskwaliteit. Als correcties niet doorgevoerd (kunnen) worden, verslechtert de gegevenskwaliteit en zijn de gegevens uiteindelijk (mogelijk) niet meer geschikt. U loopt een compliance risico (art. 36 Wbp / art 16 en 17 GDPR).
5.11	5. Gebruik van gegevens Kunnen de betrokkenen hun gegevens verwijderen of daarom vragen? Hierbij kan gedacht worden aan een reactie op verzoeken of het geven van eigen verwijderingsmogelijkheden in de eigen gegevens door middel van een informatiesysteem (waarbij wel moet vast staan dat gegevens alleen verwijderd kunnen worden door personen die dat mogen).	Nee Gegevens worden automatisch verwijderd na 4 weken (28 dagen) Advies: U loopt een verhoogd risico. Betrokkenen hebben het recht om een verzoek in te dienen voor het verwijderen van gegevens. Als er geen zwaarwegende redenen zijn om dit niet te doen, dient dit ook uitgevoerd te worden. In andere gevallen heeft de betrokkene het recht medegedeeld te worden om welke reden (deels) niet aan het verzoek wordt voldaan. U loopt hiermee een compliance risico (art. 36 Wbp / art. 16 en 17 GDPR).
6.1	6. Bewaren en vernietigen Is een bewaartermijn voor de gegevens vastgesteld? Houdt hierbij rekening met het doel waarvoor de gegevens zijn verzameld en vervolgens worden verwerkt en bedrijfsrichtlijnen en wettelijk vastgestelde bewaartermijnen zoals bijvoorbeeld in de Archiefwet, belastingwet.	Ja 28 dagen Advies: Ga verder met de volgende vraag

	Vraag	Antwoord
6.2	6. Bewaren en vernietigen Kunnen de gegevens na afloop van de bewaartermijn fysiek worden verwijderd (uit een bestand) of vernietigd (papier)? Het is niet voldoende om gegevens aan te merken als ‘verlopen’; na het aflopen van de bewaartermijn dienen deze daadwerkelijk verwijderd te worden. U dient bij de beantwoording van de vraag rekening te houden met: 1. Of het mogelijk is (delen van) de gegevens te vernietigen of te verwijderen. 2. Indien de gegevens worden vernietigd of verwijderd, of dit ongedaan kan worden gemaakt. 3. Of de gegevens anoniem kunnen worden gemaakt om ze te bewaren	Ja Gegevens worden overschreven. Na afloop toezichtstermijn wordt de schijf meervoudig overschreven (gewist). Advies: Ga verder met vraag 6.2.1
6.2.1	6. Bewaren en vernietigen Zo ja, worden de gegevens na verstrijken van de bewaartermijn op zo’n manier vernietigd of verwijderd dat ze niet meer te benaderen en te gebruiken zijn? U dient bij beantwoording rekening te houden met: 1. Of regelgeving of beleid bestaat voor vernietiging van gegevens (bijvoorbeeld archiefwet). 2. Waar (welke locatie) gegevens worden bewaard. 3. Op welk medium (papier, CD, harde schijf) gegevens worden bewaard. 4. Of deze locatie/medium zijn afgeschermd voor gebruik (bijvoorbeeld het archief). 5. Welke andere redenen bestaan om de gegevens te bewaren zoals bedrijfshistorische, wettelijke, juridische redenen.	Ja Wordt contractueel geregeld met de leverancier. Advies: Ga verder met de volgende vraag
7.1	7. Beveiligen van gegevens Is sprake van intern geformuleerd beleid over het beveiligen van informatie? Denk aan: 1. Of iemand verantwoordelijk is voor dit beleid. 2. Of wordt aangesloten bij algemene beveiligingsstandaarden. 3. Of rekening wordt gehouden met het bijzondere of gevoelige karakter van gegevens. 4. Of het beveiligingsbeleid wordt getoetst.	Ja Advies: Ga verder met de volgende vraag

	Vraag	Antwoord
7.2	7. Beveiligen van gegevens Zo ja, is duidelijk op welke wijze het project, proces of gegevensuitwisseling er voor zorg draagt dat aan de gestelde eisen in het beveiligingsbeleid voldaan gaat worden? Denk hierbij aan welke maatregelen getroffen worden om te voldoen aan het beschreven beleid (een informatiebeveiligingsplan).	Ja Advies: Indien er toch sprake is van het lekken van gegevens ga verder naar vraag 8.1
8.1	8. Datalek Is er sprake geweest van een datalek? Een datalek is een inbreuk op de beveiliging die leidt tot de vernietiging, het verlies, de wijziging of ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens. Denk aan: - Kwijtgeraakte usb-stick of GSM; - Gestolen laptop, mobiele media; - Inbraak door een hacker; - Verzending van e-mail waarin de e-mailadressen van alle geadresseerden zichtbaar zijn voor alle andere geadresseerden; - Malwarebesmetting (ook ransomware); - Brand in datacenter; en - Niet geautoriseerde toegang.	Nee Advies: U kunt stoppen.