

Data Protection Impact Assessment

[gemeente X]

[Inspectie proces X] met behulp van drones

Dienst/ organisatie	[X]
Afdeling	[X]

Initiatiefnemers template DPIA-drones	SHIELD
Projectleiders	Sven de Laaf en Iris Neeleman
Projectgroep	Gemeente Amsterdam; Gemeente Breda; Gemeente Ede; Gemeente Den Haag; Gemeente Rotterdam en Politie Carolina Bamsch; Mark van der Born; Corinne van Dijk; Martin Gebraad; Daan Groenink; Barbara Heemelaar; Stefan van der Heiden; Tudor Krook; Sven de Laaf; Hedde van der Lugt; Max van Meerten; Iris Neeleman; Hans Nouwens; Amit Poeran; Mariette Pol; Patrick Reijnen; Pim Stevens en Magdalena Simidzioski
Auteurs (Privacy officers)	Magdalena Simidzioski, Martin Gebraad, Patrick Reijnen en Barbara Heemelaar
Contactpersoon	Iris.neeleman@denhaag.nl
Versie	1.0
Datum	20-11-2025

Auteur [X]
DPIA drones [X]
Versie [X]
Versie datum [X]

Documentbeheer

Versiebeheer

Versienummer	Datum	Gewijzigd door	Wijzigingen

Bij de uitvoering van de DPIA betrokken personen

De volgende personen zijn betrokken bij de totstandkoming van deze DPIA:

Rol m.b.t. DPIA	Functie	Naam
Proceseigenaar		<verplicht>
Materiedeskundige Proces		<verplicht>
Materiedeskundige Wetgeving		<verplicht>
Facilitator/procesbegeleider DPIA		<verplicht>
Penvoerder DPIA		<verplicht>
Privacy Officer		<verplicht>
Information Security Officer		<verplicht>
I-adviseur		<verplicht>
Informatiebeheer		<verplicht>
<b.v. vertegenwoordiger verwerker>		<facultatief>
		<facultatief>

Bij de uitvoering van de DPIA gebruikte documentatie

De volgende documentatie is gebruikt bij de totstandkoming van deze DPIA:

Document	Auteur	Versie	Datum
Procesbeschrijving <verplicht>			
Privacy QuickScan (pre-DPIA) <verplicht>			
Bio Baselinetoets <verplicht>			
Bio Zelfevaluatie <optioneel>			
AP-richtlijnen m.b.t. inzet van drones Regelgeving voor drones met camera Autoriteit Persoonsgegevens	Autoriteit Persoonsgegevens	1.0	31 december 2024
DPIA Inspectie met drones voor Vergunningen en Toezicht (V&T) en Haagse Pandbrigade (HPB)	Gemeente Den Haag	1.0	15 februari 2023

Inhoud

Documentbeheer	2
Versiebeheer	2
Bij de uitvoering van de DPIA betrokken personen	2
Bij de uitvoering van de DPIA gebruikte documentatie	2
Inleiding	4
a. Onderwerp en aanleiding van de DPIA	4
b. Scope van de DPIA	4
A. Het proces in kwestie	5
1. Sturing, Toezicht en Awareness	5
2. Gegevensverwerkingen	5
Persoonsgegevens	6
3. Betrokken partijen	8
4. Verwerkingslocaties	9
5. Informatiekwaliteit	9
6. Opslagbeperking en Bewaartermijnen	9
7. Informatie bescherming	11
B. Beoordeling rechtmatigheid gegevensverwerkingen	13
8. Juridisch en beleidsmatig kader	13
AVG grondslag	13
Bijzondere persoonsgegevens	14
9. Verwerkingsdoeleinden en doelbinding	15
10. Noodzaak en evenredigheid van de verwerking	16
11. Transparantie	16
12. Rechten van Betrokkenen	17
C. Risicoscenario's, gevolgen en beschermings- maatregelen	18
D. Maatregelen en Restrisco's	26
Akkoordverklaring Proceseigen(a)r(en)/gemandateerde(n)	27
Advies Functionaris Gegevensbescherming (FG)	28

Inleiding

a. Onderwerp en aanleiding van de DPIA

Deze DPIA heeft betrekking op het proces inspectie met behulp van drones, waarbij foto's, video's of andere scans worden gemaakt van het te inspecteren object. Hierbij kan het gaan om de volgende situaties:

- Inspectie van een bouwwerk in het kader van toezicht op de naleving van de omgevingswet
- Inspectie van de bouwkundige staat van objecten zoals bruggen, kades en oevers, lichtmasten, sluisdeuren, gebouwen en beschoeiingen. Deze objecten vallen onder de zorgplicht van de gemeente.
- [anders]

Door middel van de QuickScan (pre-DPIA) [van <datum>] is vastgesteld dat dit proces waarschijnlijk een verhoogd risico oplevert voor betrokkenen van wie persoonsgegevens worden verwerkt, omdat er met de inzet van drones sprake is van cameratoezicht en dus op grond van artikel 35 AVG het uitvoeren van een DPIA verplicht is.

b. Scope van de DPIA

In scope

De volgende onderdelen c.q. gegevensverwerkingen vallen binnen de scope van deze DPIA:

- Gegevensverwerkingen die voortvloeien uit de inzet van drones, zoals het vluchtplan, beeldmateriaal, live beelden en logs van de drone.
- [anders]

Buiten scope

De volgende onderdelen c.q. gegevensverwerkingen vallen buiten de scope van deze DPIA:

- De verwerking van persoonsgegevens voor het proces waarbij er geen sprake is van de inzet van drones
- [anders]

A. Het proces in kwestie

1. Sturing, Toezicht en Awareness

Beschrijf hoe rollen en verantwoordelijkheden op het gebied van privacy zijn belegd binnen de dienst(en). Beschrijf ook wat de mate van AVG-bewustzijn is binnen de dienst en wat er wordt ondernomen om dit op peil te houden.

Analysevragen

- Wie is verantwoordelijk voor de verwerking?
- Zijn de rollen en verantwoordelijkheden duidelijk (RASCI)
- Worder er regulier awareness sessies georganiseerd?

De verantwoordelijke voor deze verwerking is de gemeente [Naam]. De gemandateerde verwerkingsverantwoordelijke namens de gemeente is [directeur/afdelingshoofd].

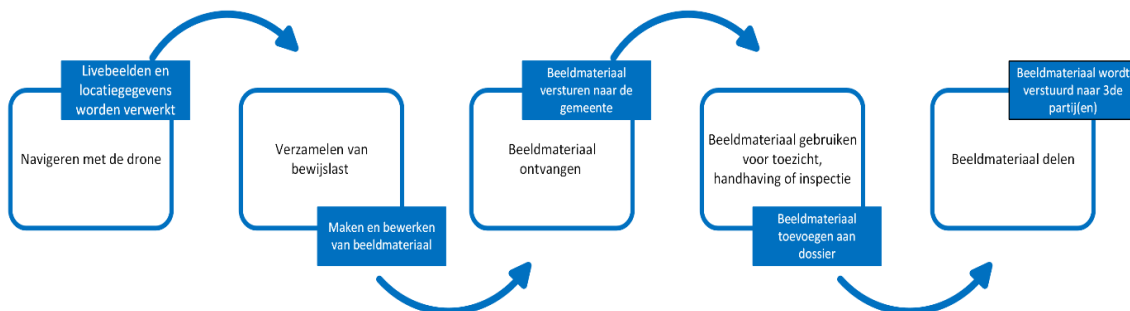
De rollen en verantwoordelijkheden zijn duidelijk vastgelegd.

2. Gegevensverwerkingen

Beschrijf alle voorgenomen gegevensverwerkingen/Processtappen en het doel van de verwerking. Maak hierbij een duidelijk onderscheid tussen het verzamelen en het verstrekken van persoonsgegevens, zodat in het tweede deel van de DPIA bepaald kan worden of voor beide verwerkingen wel een rechtsgrond bestaat. Benoem ook of er sprake is van bijzondere toepassingen, zoals geautomatiseerde besluitvorming (Algoritmen), profilering of statistisch onderzoek middels een BI-voorziening of het UDP. Desgewenst kan een stroomschema van de gegevensverwerkingen worden toegevoegd. Als er sprake is van een verdere verwerking dient ook het oorspronkelijke doeleinde te worden opgenomen. Voeg aanvullende informatie toe in het analyseveld.

Het proces betreft inspectie en toezicht op objecten in de buitenruimte met behulp van drones. Het doel van de DPIA is om risico's in het proces te identificeren, om te kijken op welke manier drone-inspectie verschilt van een reguliere inspectie en welke maatregelen er nodig zijn om de privacy van burgers te waarborgen.

- Beschrijving van de processtappen



Navigeren met drone

Navigeren met een drone omvat verschillende technologieën en methoden, waaronder GPS, sensoren en visuele systemen. Een drone kan autonoom vliegen door vooraf geprogrammeerde routes te volgen of

handmatig worden bestuurd door een piloot. Tijdens het navigeren verzamelt de drone continue gegevens om zijn positie, hoogte en omgeving te bepalen. Deze gegevens omvatten vaak GPS-coördinaten, hoogtemetingen, en visuele informatie vanuit de camera's aan boord van de drone. Bij het verwerken van deze gegevens kunnen verschillende persoonsgegevens worden vastgelegd. Dit zijn onder andere:

- Beeldmateriaal van personen die zich in de buurt van de drone bevinden, vastgelegd door de camera's.
- Locatiegegevens, zoals GPS-coördinaten van de drone en eventueel van objecten of personen in de buurt.
- <Voeg toe>

Verzamelen van beeldmateriaal

Tijdens inspecties van bouw- of andere objecten in de buitenruimte worden drones ingezet om specifiek beeldmateriaal te verzamelen dat essentieel is voor de inspectie. De drones zijn uitgerust met geavanceerde camera's die zowel foto's als video's kunnen maken. De piloot van de drone bestuurt het toestel handmatig en autonoom naar de locatie van het te inspecteren object. Tijdens de vlucht wordt continu livebeeld gebruikt om de nauwkeurigheid van de vlucht te waarborgen en de juiste beelden te verkrijgen. Deze livebeelden dienen puur ter navigatie en worden zodoende niet opgeslagen onder meer om de privacy van burgers te beschermen. Pas bij het te inspecteren object wordt beeldmateriaal opgenomen.

[Verder specificeren hoe beeldmateriaal wordt verzameld]

Na het verzamelen van het beeldmateriaal door de drone, wordt dit eerst opgeslagen op een SD-kaart in de drone zelf. Zodra de drone terugkeert naar de basis, worden de beelden overgebracht naar een beveiligde computer voor verdere verwerking. Bij de verdere verwerking worden alle persoonlijke gegevens, zoals gezichten van mensen en kentekens van voertuigen, (automatisch of handmatig) geblurd om de privacy te waarborgen.

Beeldmateriaal ontvangen en opslaan

[invullen, zie voorbeelden in werkinstructie]

Beeldmateriaal gebruiken voor inspectie

[invullen, zie voorbeelden in werkinstructie]

Beeldmateriaal delen

[invullen, zie voorbeelden in werkinstructie]

- Beschrijving van de verschillende type inspecties met drones
<voeg de beschrijving toe>

Persoonsgegevens

Beschrijf alle persoonsgegevens die worden verwerkt per processtap. Classificeer deze persoonsgegevens naar: gewoon, gevoelig, bijzonder, strafrechtelijk en wettelijk identificatienummer. Dit is verder uitgewerkt in de werkinstructie. Herhaal deze stap als er meerdere categorieën

Processtap: Navigeren met drone

Persoonsgegevens	Type persoonsgegevens	Bron	Noodzaak	Doel
Zicht op voorgevel vanaf openbare weg	Normale persoonsgegevens	Drone operator	Livebeelden zijn noodzakelijk ter navigatie. Beelden worden niet vastgelegd	Drone naar juiste locatie/positie brengen

Persoonsgegevens	Type persoonsgegevens	Bron	Noodzaak	Doel
Bewoners, omwonenden en voorbijgangers in de buurt van het object. [of andere]	Normale persoonsgegevens	Drone operator	Livebeelden zijn noodzakelijk ter navigatie. Beelden worden niet vastgelegd	Drone naar juiste locatie/positie brengen
Vluchtgegevens, zoals locaties, route, hoogte etc. (niet: de videobeelden).	Normale persoonsgegevens	Drone operator	Vluchtgegevens ter navigatie van de drone worden alleen in de drone vastgelegd (verplicht)	Drone naar juiste locatie/positie brengen
Zicht op de tuin/ achtergevel & zicht in de woning. [of andere]	Gevoelige persoonsgegevens	Drone operator	Livebeelden zijn noodzakelijk ter navigatie. Beelden worden niet vastgelegd	Drone naar juiste locatie/positie brengen

Processtap: Verzamelen van beeldmateriaal

Persoonsgegevens	Type persoonsgegevens	Bron	Noodzaak	Doel
Foto's van het te inspecteren object. Kunnen persoonsgegevens bevatten bijvoorbeeld wanneer er zicht is op de tuin/ achtergevel & zicht in de woning.	Normale/ gevoelige persoonsgegevens	Drone operator/ SD kaart	Ter inspectie	Uitvoeren van gemeentelijke taken

Processtap: Beeldmateriaal ontvangen en opslaan

Persoonsgegevens	Type persoonsgegevens	Bron	Noodzaak	Doel
[Foto's worden na overdracht door gemeente gebruikt om inspecties uit te voeren. Na bewerking komen hier geen direct identificerende persoonsgegevens in voor. Hooguit zou er nog herleidbaarheid bestaan op basis van het te inspecteren object dat in beeld is gebracht].	Normale (persoons)gegevens	Gemeente [Naam]	Ter inspectie	Uitvoeren van gemeentelijke taken [Vul aan met andere doelen] [Het controleren van vergunningsaanvragen en toezichthouden op de uitvoering (bouw)] [Het controleren van objecten na meldingen] Etc.

3. Betrokken partijen

Benoem alle organisaties die betrokken zijn bij de voorgenomen gegevensverwerking. Deel deze organisaties in onder de rollen: verwerkingsverantwoordelijke, gezamenlijke verwerkingsverantwoordelijke, verwerker, sub verwerker, verstrekker, ontvanger en derde. Benoem ook welke functies/afdelingen binnen deze organisaties toegang krijgen tot persoonsgegevens. Voeg aanvullende informatie toe in het analyseveld.

Naam	Rol	Functie/ afdeling	Persoonsgegevens
Gemeente [naam]	Verwerkings-verantwoordelijke		Beelden als resultaat van de dronevlucht.
Drone Operator	Verwerker (voor de activiteit opnames maken tbv inspectie)		Beelden en foto's.
Drone Operator	Verwerkingsverantwoordelijke (voor de activiteit vliegen) en verwerker		Live navigatiebeelden, vluchtgegevens.
Leverancier Cloud	(sub)Verwerker		Beelden (al dan niet geblurd)
Beheerder van drone software	[verwerker + checken of die ook zelfstandig verantwoordelijk is]		

Analysevragen

- Is er sprake van een samenwerkingsverband?
- Is er een convenant opgesteld? (NB: Een convenant is geen rechtsgrond.)
- Heeft Information Security een leverancierstoets uitgevoerd?
- Zo ja, voldoet deze leverancier aan de gemeentelijke standaarden (denk o.a. aan ISO/NEN/ISEA/SOC verklaringen)?
- Wat is de rol van de wederpartij?
- Moet er een verwerkersovereenkomst worden gesloten?
- Is er een verwerkersovereenkomst, een gezamenlijke verwerkersovereenkomst, GUO of GLO afgesloten?
- Heeft Information Security bijlage 2 van de verwerkersovereenkomst beoordeeld?
- Vindt monitoring plaats op de naleving van de overeenkomst?
- Is er een procedure overeengekomen die toeziet op de bewaartermijn en de mogelijke vernietiging of archivering aan het einde van de bewaartermijn.

<Conclusie over samenwerkingsverbanden, verwerkingsverantwoordelijke, ..>

4. Verwerkingslocaties

Gegevensverwerkingen	Verwerkingslocaties	Doorgiftemechanisme
Live navigatiebeelden	Nederland (of EER)	n.v.t.
Foto's	Nederland (of EER)	n.v.t.
Videobeelden	Nederland (of EER)	n.v.t.
Vluchtgegevens	Nederland (of EER)	n.v.t.

Benoem in welke landen de voorgenumen gegevensverwerkingen plaatsvinden. Beschrijf het doorgiftemechanisme (bv. Adequaateheidsbesluit) dat van toepassing is wanneer verwerkingslocaties buiten de Europese Economische Ruimten bevinden. Voeg aanvullende informatie toe in het tekstveld.

De gegevens die door drones worden verzameld, worden uitsluitend opgeslagen binnen de Europese Economische Ruimte (EER). Indien drones van fabrikanten buiten de EER worden ingezet, worden er maatregelen genomen om te garanderen dat de verzamelde data de EER niet verlaat. Deze maatregelen omvatten onder andere het gebruik van versleuteling en veilige verbindingen voor dataoverdracht.

[Aangeven of er sprake is van grensoverschrijdend gegevensverkeer. Vindt het beheer en opslag in de EU/EER plaats?]

5. Informatiekwaliteit

Beschrijf welke maatregelen genomen zijn om te borgen dat persoonsgegevens juist, volledig en actueel zijn.

Analysevragen

- Hoe worden de persoonsgegevens blijvend juist, volledig en actueel gehouden?
- Hoe vindt controle op datakwaliteit plaats (vooraf, achteraf)?
- Vinden er handmatige controles of reviews plaats?
- Worden persoonsgegevens middels de BRP gecontroleerd?
- Wordt een vier-ogenprincipe in de processtappen toegepast?

<Voeg hier de beschrijving toe>

6. Opslagbeperking en Bewaartermijnen

Bepaal de bewaartermijnen van de persoonsgegevens aan de hand van de gegevensverwerkingen en de verwerkingsdoeleinden. Onderbouw dat de gegevens niet langer worden verwerkt dan noodzakelijk voor het doel. Onderscheid de termijn voor het primair proces en de bewaartermijn onder de Archiefwet. Geef aan of bewaartermijn geautomatiseerd is ingeregeld of dat er een ander proces voor is ingericht. Beschrijf wie toeziet op de bewaartermijn en de mogelijke vernietiging of archivering aan het einde van de bewaartermijn.

Beschrijf welke mogelijkheden van anonimiseren of pseudonimiseren worden toegepast.

Persoonsgegevens worden direct (of zo snel mogelijk) geblurd en daardoor geanonimiseerd. De (geblurde) beelden van de objecten mogen conform de Archiefwet 5 jaar worden bewaard.

Gegevensverwerking	Bewaartermijn	Motivatie bewaartermijn (indien wettelijk, wetsartikel benoemen))
Livebeelden	Niet bewaard	N.v.t. Beelden van de vlucht worden niet bewaard.
Vluchtgegevens (niet de beelden)	5 jaar	De vluchtgegevens worden 4 tot 5 jaar bewaard om te kunnen voldoen aan inspecties van de Inspectie Leefomgeving en Transport . ⁸
Foto's voor inspectie/controle	[Bewaartermijn van inspectierapport proces]	Bewaartermijn is gelijk aan die van het inspectierapport, omdat de foto's daar integraal onderdeel van uitmaken.

Analysevragen

- Stel met Informatiebeheer vast welke bewaartermijnen en procedures van toepassing zijn. Denk aan de Archiefwet, de Adviesnota Bewaartermijnen en de Selectielijst.
- Hoe worden persoonsgegevens bewaard en worden persoonsgegevens die niet langer nodig zijn daadwerkelijk verwijderd?
- Is er een retentiebeleid opgesteld?
- Welke controles vinden plaats op de naleving van het retentiebeleid?
- Hoeveel databases worden gebruikt voor de verwerking? Welke documenten worden integraal opgeslagen? Is het noodzakelijk deze documenten te behouden of worden de relevante gegevens tevens in een systeem vastgelegd?
- Worden persoonsgegevens op meerdere plekken naast elkaar opgeslagen? B.v.: G-schijf, systeem en mail? Zo ja, waarom en waar?
- Is het technisch mogelijk persoonsgegevens te verwijderen?
- Welke procedure wordt gevolgd om gegevens na het verstrijken van de bewaartermijn te vernietigen?
- Hoe vindt de vernietiging plaats? Gebeurt dit handmatig of (semi) geautomatiseerd?
- Hoe kan worden aangetoond dat de persoonsgegevens zijn vernietigd?
- Hoe wordt omgegaan met bestanden waarin persoonsgegevens zitten met verschillende bewaartermijnen? Kan een gedeelte van de gegevens worden verwijderd?
- Hoe wordt omgegaan met het verwijderen van persoonsgegevens die zijn opgenomen in log- en/of back-up bestanden?
- In hoeverre kan het doel van de verwerking ook met geanonimiseerde of gepseudonimiseerde gegevens worden bereikt?
- Worden gegevens in het proces/de verwerking geanonimiseerd? (Licht toe)
- Worden gegevens in het proces/de verwerking gepseudonimiseerd? (Licht toe)
- Op welk aggregatieniveau worden gegevens gebruikt in rapportages? Zijn deze gegevens herleidbaar tot persoonsniveau?

[toelichting]

7. Informatie bescherming

Binnen de gemeente is de Baseline Informatiebeveiliging Overheid (BIO) het basishoofdnormenkader voor informatiebeveiliging. Door middel van de BIO Baseline toets wordt voor de applicatie(s) die het proces ondersteunen het niveau van Beschikbaarheid, Integriteit en Vertrouwelijkheid van data vastgesteld. Om persoonsgegevens adequaat te beschermen moeten er passende beveiligingsmaatregelen genomen worden. Middels een BIO baselinetoets wordt bepaald welk basisbeveiligingsniveau van toepassing is. De uitkomst dient als input voor de eventueel te nemen additionele beveiligingsmaatregelen. Standaard dienen de onderstaande 4 vragen beantwoord te worden. Zolang er geen BIO baseline toets heeft plaatsgevonden is de bescherming van persoonsgegevens niet adequaat onderzocht en zal een negatief advies op de DPIA volgen. Wanneer de applicaties niet worden meegenomen in de BIO zelfevaluatie is een duurzame bescherming van gegevens niet geborgd. Ook deze bevinding zal leiden tot een negatief advies. Wanneer de rapportages niet beschikbaar zijn, kan de gemeente niet aantonen dat zij voldoet aan het normenkader, De proceseigenaar zal zich in dat geval moeten committeren aan een harde opleverdatum.

Analysevragen

- Heeft er een BIO baseline toets plaatsgevonden op de applicaties die het proces ondersteunen? (Geef dit aan voor iedere applicatie)
- Zijn de ondersteunende applicaties meegenomen in de BIO zelfevaluatie? (Geef aan voor iedere applicatie)
- Zijn de rapportages/verbeterplannen die voortkomen uit de zelfevaluatie beschikbaar?
- Hebben de rapportages/verbeterplannen gevolgen die in de DPIA meegenomen moeten

Op basis van de uitgevoerde BIO baseline toetsen heeft dit proces een vertrouwelijkheid van BBN 1 niveau omdat er in principe geen persoonsgegevens verwerkt worden. Echter kan het zijn dat voor sommige processen die gebruik maken van drones wel persoonsgegevens verwerkt worden. Daarom gaan wij er van uit dat processen waarbij drones ingezet worden standaard een BBN 2 niveau hebben en alle informatiebeveiligingsmaatregelen voor dit BBN-niveau van toepassing zijn.

Zelfs wanneer de eerste drie vragen positief beantwoord is het zinvol de bescherming te toetsen op autorisatie en logbestanden. Controleer wat in de Bio baseline toets/rapportage zelfevaluatie staat.

Autorisatie

Alleen bevoegde gebruikers mogen toegang hebben tot de informatiesystemen en diensten die ze voor de uitvoering van hun taken nodig hebben en om onbevoegde toegang tot informatiesystemen te voorkomen.

Logging

Activiteiten die gebruikers en beheerders uitvoeren met persoonsgegevens moeten worden vastgelegd in logbestanden. Hetzelfde geldt voor andere relevante gebeurtenissen, zoals pogingen om ongeautoriseerd toegang te krijgen tot persoonsgegevens en verstoringen die kunnen leiden tot verminking of verlies van persoonsgegevens. De logbestanden moeten periodiek gecontroleerd worden op indicaties van onrechtmatige toegang of onrechtmatig gebruik van de persoonsgegevens en waar nodig wordt actie ondernomen.

Analysevragen

- Is er een autorisatiematrix?
- Is er een procedure die periodiek toegangsrechten controleert (inclusief mogelijke opvolging van de bevindingen)?
- In hoeverre worden activiteiten die gebruikers en beheerders uitvoeren met persoonsgegevens vastgelegd in logbestanden?
- In hoeverre worden logbestanden periodiek gecontroleerd op indicaties van onrechtmatige toegang of onrechtmatig gebruik van de persoonsgegevens?
- Welke acties worden genomen op indicaties van onrechtmatige toegang/onrechtmatig gebruik?

B. Beoordeling rechtmatigheid gegevensverwerkingen

8. Juridisch en beleidsmatig kader

Benoem per gegevensverwerking/processtap alle wet- en regelgeving en beleid met mogelijke gevolgen. De AVG hoeft niet genoemd te worden. Voeg zo nodig aanvullende informatie toe in het tekstveld.

Gegevensverwerkingen/ Processtappen	Juridisch en/of beleidsmatig kader	Wetsartikelen
1. live navigatiebeelden	EU-Verordening (EU) 2019/945 en Uitvoeringsverordening (EU) 2019/94 inzake drones	
2. foto's maken en bewerken	wettelijke grondslag (bijvoorbeeld omgevingswet)	
3. foto's gebruiken voor inspectie en toezicht	wettelijke grondslag (bijvoorbeeld omgevingswet)	
4. delen van foto's	[wettelijke grondslag of verenigbaarheidstoets]	

Er zijn naast de AVG ook andere wettelijke kaders die van toepassing zijn bij het gebruik van drones.

Er bestaat sectorspecifieke wetgeving voor de inzet van drones:

- EU-Verordening (EU) 2019/945 inzake drones

De EU-Verordening (EU) 2019/945 stelt eisen aan de technische specificaties en productie van drones. Deze verordening heeft als doel om de veiligheid, beveiliging en milieubescherming te waarborgen bij het gebruik van drones. Het bevat regels over het ontwerp, de vervaardiging en het onderhoud van drones, alsmede de verplichtingen van fabrikanten en operators.

- Uitvoeringsverordening (EU) 2019/947 inzake drones.

De EU Uitvoeringsverordening (EU) 2019/947 betreft de operationele eisen voor het gebruik van drones. Deze verordening is van toepassing op zowel recreatief als commercieel gebruik van drones en omvat regels over de registratie van drone-exploitanten, certificering van piloten, operationele beperkingen en veiligheidsmaatregelen.

[bewijs dat leverancier voldoet + certificeringen opvragen van de drone piloot]

AVG grondslag

Bepaal op welke rechtsgronden de gegevensverwerkingen worden gebaseerd. Iedere rechtsgrond moet aan bepaalde voorwaarden voldoen, voeg in de toelichting op de rechtsgrond toe hoe aan deze voorwaarden wordt voldaan. Geef zo nodig aanvullende informatie in het analyseveld.

Gegevensverwerkingen/ Processtappen	Rechtsgrond	Toelichting op de rechtsgrond
1. live navigatiebeelden	Algemeen belang	De gemeente heeft de taak om te beslissen over een omgevingsvergunning op grond van de Omgevingswet.

Gegevensverwerkingen/ Processtappen	Rechtsgrond	Toelichting op de rechtsgrond
		De gemeente heeft de taak om te toezicht te houden op de openbare ruimte op grond van de [wet].
2. foto's maken en bewerken	Algemeen belang	De gemeente heeft de taak om te beslissen over een omgevingsvergunning op grond van de Omgevingswet. De gemeente heeft de taak om te toezicht te houden op de openbare ruimte op grond van de [wet].
	Gerechtvaardigd belang	Met de inzet van drones heeft de gemeente een gerechtvaardigd belang omdat de fysieke inspectie (deels) overbodig wordt en de werknemer niet onnodig wordt blootgesteld aan veiligheidsrisico's. De gemeente heeft een taak in het kader van goed werkgeverschap noodzakelijke voorzieningen te treffen om medewerkers goed en veilig te laten werken (zie: artikel 125 ambtenarenwet).
3. foto's gebruiken voor inspectie en toezicht	Algemeen belang	De gemeente heeft de taak om te beslissen over een omgevingsvergunning op grond van de Omgevingswet. De gemeente heeft de taak om te toezicht te houden op de openbare ruimte op grond van de [wet].
4. Delen van foto's van de objecten met [derde partij]		
[Andere processtappen]	<Algemeen belang of Wettelijke verplichting>	

Bijzondere persoonsgegevens

Het verwerken van bijzondere of strafrechtelijke persoonsgegevens is in principe verboden. Verwerking is pas mogelijk wanneer een uitzonderingsgrond van toepassing is. Beoordeel of een van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing is. Bij verwerking van een nationaal identificatienummer (zoals BSN), beoordeel of dit is toegestaan. Voeg zo nodig aanvullende informatie toe in het tekstveld.

Analysevragen

-Wordt in de applicaties die het proces ondersteunen gebruik gemaakt van vrije tekstvelden (die bijzondere persoonsgegevens kunnen bevatten)?

Als er bijzondere persoonsgegevens worden verwerkt:

-Is een van de uitzonderingsbepalingen van artikel 9 van toepassing?

-Is een van de uitzonderingsbepalingen van artikelen 22-30 van de UAVG van toepassing?

Het doel van de inzet van drones is primair gericht op het inspecteren van objecten in de openbare ruimte en niet op het verwerken van bijzondere persoonsgegevens. Hierdoor is het verwerken van bijzondere persoonsgegevens niet noodzakelijk.

[Niet van toepassing, tenzij]

Gegevensverwerkingen/ Processtappen	Type bijzonder/strafrechtelijk gegeven/ BSN	Uitzonderingsgrond
1.		

9. Verwerkingsdoeleinden en doelbinding

Als de persoonsgegevens voor een ander doel worden verwerkt dan oorspronkelijk verzameld, beoordeel of deze verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld. Voeg in het tekstveld de verenigbaarheidstoets en aanvullende informatie toe. Indien er sprake is van verdere verwerking voor statistieken of voor wetenschappelijk onderzoek hoeft er geen verenigbaarheidstoets uitgevoerd te worden.

Gegevensverwerking	Persoonsgegevens	Doeleinde	Oorspronkelijk doeleinde

Analyse

- Is het doel van de verwerking van persoonsgegevens voldoende SMART omschreven en vastgelegd?

- Worden alleen die gegevens vastgelegd die noodzakelijk zijn voor het doel van de verwerking? Welke zijn dat niet?

N.B. De doelbindingstoets kan achterwege blijven als de gegevensverstrekking wettelijk verplicht is of als de betrokkene toestemming heeft gegeven (waarbij geldt dat toestemming in casu vaak niet aan de orde/mogelijk is).

De primaire doelstelling van gemeente [X] bij de inzet van de drone is het maken van foto's ten behoeve van het uitvoeren van haar inspectietaak en vastleggen van beeldmateriaal. Door middel van de inzet van de drone kunnen objecten gemakkelijker en beter in beeld worden gebracht. De drone dient voor inspecties van buitenaf als alternatief voor het langs sturen van een inspecteur op locatie.

10. Noodzaak en evenredigheid van de verwerking

Beoordeel of de voorgenomen gegevensverwerkingen (dus niet de individuele categorieën van gegevens!) noodzakelijk en evenredig zijn voor het verwezenlijken van de verwerkingsdoeleinden. Denk hierbij b.v. aan cameratoezicht, fraudeonderzoek en kentekenherkenning.

Ga hierbij in ieder geval in op:

- a. Proportionaliteit: staat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden?
- b. Subsidiariteit: kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkenen minder nadelige wijze, worden verwezenlijkt?

Analysevragen

- Is er sprake van een wettelijke plicht of een wettelijke bevoegdheid? Bij een wettelijke plicht heeft de wetgever de noodzakelijkheidstoets al gedaan.
- Hoe is gewaarborgd dat de minimale/toereikende hoeveelheid gegevens wordt verzameld om het doel te bereiken?
- Zijn er andere manieren mogelijk om het doel te bereiken, die minder ingrijpend zijn voor de privacy van de betrokkenen?

[toelichting]

11. Transparantie

Beschrijf hoe betrokkenen geïnformeerd worden over wat de gemeente met hun gegevens doet en of de algemene privacy verklaring voldoet.

- Is de verwerking opgenomen in de generieke privacyverklaring?
- Voldoet de generieke verklaring voor het specifieke proces?
- Zo nee: op welke manier wordt de betrokkene dan wel geïnformeerd? Dit kan bijvoorbeeld via een specifieke privacyverklaring, maar zou ook een folder of een toelichting kunnen zijn.
- Is voor alle verwerkingen relevante informatie verstrekt aan de betrokkene(n)? Zijn het gebruik, het doel en de manier van verwerking duidelijk kenbaar gemaakt?

Bij inspecties worden bewoners en gebruikers geïnformeerd zoals bij een traditionele controle, inclusief uitleg over dronegebruik. Buurtbewoners krijgen een schriftelijke notificatie over het gebruik van drones. Voor inspecties in openbare ruimtes worden betrokkenen via informatieborden met QR-codes geïnformeerd, waar ze details zoals de privacyverklaring kunnen vinden. Het gebied wordt afgezet met pionnen en waarschuwingsborden, en zowel het werkvoertuig als de drone zijn duidelijk gemarkeerd met het gemeentelogo. Bewoners krijgen ook informatie via flyers en brieven, en kunnen de inspectie volgen op een scherm naast het voertuig, wat helpt bij een positieve beeldvorming. Daarnaast wordt er indien van toepassing contact opgenomen met de verkeersleiding van het dichtstbijzijnde vliegveld voor veilige vluchtuitvoering, en wordt het gemeentelijke telefoonnummer ingelicht.

Aanbevelingen:

- Landelijk registratiesysteem.
- Gemeentelijke landingspagina voor dronebeelden.
- Vluchten aankondigen via onlinekanalen.
- Iemand ter plaatse voor vragen.
- Drones markeren met gemeentelogo's en kleuren.
- Gemeentelijk KCC en politie informeren volgens AP-richtlijnen.
- + standaard bord net zoals voor de camera's

12. Rechten van Betrokkenen

Beschrijf de procedure waarmee invulling wordt gegeven aan de rechten van de betrokkenen en welke partij verantwoordelijk is voor de uitvoering van de procedure. Als de rechten van de betrokkene worden beperkt, beschrijf op grond van welke wettelijke uitzondering dat is toegestaan. Toets of de rechten in praktijk uitgevoerd kunnen worden.

- Is een van de uitzonderingsbepalingen van artikel 23 AVG van toepassing?
- Is de uitzonderingsbepaling van artikel 41 UAVG van toepassing?
- Hoe kunnen betrokkenen hun rechten op grond van de AVG uitoefenen?
- Hoe worden verzoeken van een betrokkenen (o.a. inzage, wijziging of verwijdering van gegevens) afgehandeld?
- Hoeveel tijd neemt dit in beslag (maximale termijn in de AVG is 1 maand)?
- Is functionaliteit beschikbaar die de organisatie bij een inzageverzoek ondersteunt bij het genereren van een overzicht van persoonsgegevens?

[Beschrijving procedure]

C. Risicoscenario's, gevolgen en beschermingsmaatregelen

Kernonderdeel van de DPIA is het inschatten van mogelijke risico's voor betrokkenen die voortkomen uit de beoogde gegevensverwerking. Op grond van overweging 75 AVG kunnen de risico's voor de rechten en vrijheden van betrokkenen wanneer zij optreden, resulteren in ernstige lichamelijke, materiële of immateriële schade. Denk hierbij aan gevolgen zoals:

- Discriminatie, stigmatisering en uitsluiting;
- (Blootstelling aan) identiteitsdiefstal of -fraude;
- Financiële verliezen;
- Reputatie- of anderszins relationele schade;
- Verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens;
- Ongeoorloofde ongedaanmaking van pseudonimisering;
- Of enig ander aanzienlijk economisch of maatschappelijk nadeel voor de natuurlijke persoon in kwestie;

Voor het optreden van risico's moet naast de **impact** ('wat is de ernst van de schade voor betrokkene?') beoordeeld worden hoe groot de **kans** is dat een risico optreedt ('hoe groot is de kans dat deze schade zich voordoet?'). Voor de beoordeling van de kans van optreden is de kwaliteit van de verwerkingsomgeving (de situatie) maatgevend. Hoe beter de genomen maatregelen zijn, hoe kleiner de kans van optreden.

Het risico moet worden bepaald op basis van een objectieve beoordeling. Hierbij moet worden gekeken naar de aard, het toepassingsgebied, de context en de doeleinden van de verwerking.

Het risiconiveau wordt als volgt vastgesteld: $\text{Kans} \times \text{Impact} = \text{Risico}$. Ieder element krijgt een waarde en een kleur toegekend die de status van het element omschrijft, namelijk (1) **laag**, (2) **gemiddeld**, (3) **hoog**.

Ernst van gevolgen Kans van optreden	Klein	Middelgroot	Groot
Laag	Risico Laag	Risico Laag	Risico Middel
Middel	Risico Laag	Risico Middel	Risico Hoog
Hoog	Risico Middel	Risico Hoog	Risico Hoog

In dit hoofdstuk wordt per privacy thema beschreven welke risico's (scenario's) gesignaleerd worden, wat de gevolgen zijn voor de betrokkene(n), hoe groot de kans is dat de gevolgen intreden en welke maatregelen genomen kunnen worden om verwerkingsrisico's weg te nemen of te mitigeren.

[Bepaal de risicoscenario's. Zie voor veel voorkomende scenario's de lijst die beschikbaar is in de Werkinstructie DPIA Drones, hoofdstuk 1.3.]

[Let op! Deze lijst is niet limitatief. Voeg ook risico scenario's toe op basis van jouw eigen analyse]

[Benoem per privacy thema het risicoscenario en beschrijf kort de gevolgen voor de betrokkene(n).

Hoe groot is de kans dat dit risico intreedt? Geef een onderbouwing.

Omschrijf welke maatregelen genomen kunnen worden, wat het restrisico is en licht dit toe.]

• Sturing en Toezicht

Risico: Onvoldoende vastgelegd rondom sturing en toezicht

Wat zijn de gevolgen voor betrokkene(n)?	Dit kan diverse gevolgen hebben voor de betrokkene zoals		
Inschatting Impact	☐ Laag	☐ Midden	☐ Hoog
Onderbouwing:			
Kans op intreden	☐ Laag	☐ Midden	☐ Hoog
Onderbouwing:			
Risico (impact x kans)	☐ Laag	☐ Midden	☐ Hoog
Aanvullende maatregelen?	Zorg dat bij de dienst/afdeling een verantwoordelijke is voor de inzet van drone-technologie. Deze heeft in ieder geval de volgende taken: • Maken en bewaken van afspraken met de drone operator; • Zorgen bij de planning van de vluchten dat ook de noodzakelijke transparantiemaatregelen worden genomen (o.m. informeren politie, informeren 1407); • Periodiek (bv jaarlijks) toetsen samen met de privacy officer of de voorgestelde maatregelen uitgevoerd worden en/of procesverbeteringen noodzakelijk zijn. • Zorg dat de inzet van drones ook wordt opgenomen in het register van verwerkingen. • Zorg dat bij wijziging van de scope van drone-inzet (bijvoorbeeld gebruik voor andere doelen) en ook bij een wezenlijk andere aanpak (bijvoorbeeld vliegen buiten direct zicht van de piloot (BVLOS)) de DPIA wordt aangepast of herzien.		
Restrisico	☐ Laag	☐ Midden	☐ Hoog
Toelichting:			

• Betrokken Partijen

Risico: Onvoldoende afspraken gemaakt en vastgelegd met de verwerkers.

Wat zijn de gevolgen voor betrokkene(n)?	Dit kan diverse gevolgen hebben voor de betrokkene zoals bijv. dat de beelden door de leverancier voor andere doeleinden ingezet worden of onvoldoende beveiligd zijn waardoor de kans op een datalek hoog is.		
Inschatting Impact	☐ Laag	☐ Midden	☐ Hoog
Onderbouwing:			
Kans op intreden	☐ Laag	☐ Midden	☐ Hoog
Onderbouwing:			
Risico (impact x kans)	☐ Laag	☐ Midden	☐ Hoog
Aanvullende maatregelen?	• Contracteer een drone-operator die conform de Uitvoeringsverordening (EU) 2019/94 inzake drones gecertificeerd is voor de risicoklasse 'specific'. Laat de drone-operator		

	aantoonbaar maken dat zij ook voldoende uitvoering geven aan informatiebeveiliging en privacy. - Leg instructies vast op de voor de noodzakelijke verwerkingen: - Drone in zicht van de piloot (Vision Line of Sight); - Vlieghoogte voor het nemen van foto's ruim boven object (50-70 meter); - Kwaliteit van beelden (camera) en kwalificatie van de cameraman; - Te nemen foto's op instructie van een deskundige van de gemeente; - Beeldbewerking van foto's om niet noodzakelijke gegevens te verwijderen/blurren; - Vastleggen van type gegevens die altijd verwijderd moeten worden (bv personen, kentekenplaat voertuig); - Verwijderen van foto's na versturen van foto's naar de gemeente; - Verwijderen van beelden van vlucht, na de vlucht. - Maak afspraken met politie op het doorgeven van inspectievluchten. - Maak afspraken met 14070 / +31703533000 op het doorgeven van inspectievluchten.		
Restrisico	☐ Laag	☐ Midden	☐ Hoog
Toelichting:			

• Verwerkingslocaties

Risico: Data wordt buiten de EER verwerkt als er gebruik gemaakt wordt van drone fabrikanten buiten de EER.

Wat zijn de gevolgen voor betrokkene(n)?	Er bestaat een mogelijkheid dat de data die verzameld wordt met een drone die buiten de EER geproduceerd is, ook buiten de EER verwerkt wordt.		
Inschatting Impact	☐ Laag	☐ Midden	☐ Hoog
Onderbouwing:			
Kans op intreden	☐ Laag	☐ Midden	☐ Hoog
Onderbouwing:			
Risico (impact x kans)	☐ Laag	☐ Midden	☐ Hoog
Aanvullende maatregelen?	- Zorg dat de data de EER niet verlaat. - Als dit wel het geval is, zorg voor additionele afspraken met de derde partij(en) conform de AVG.		
Restrisico	☐ Laag	☐ Midden	☐ Hoog
Toelichting:			

• Informatiekwaliteit

Risico: Er worden verkeerde conclusies gemaakt op basis van foutieve informatie die verzameld is met de drone.

Wat zijn de gevolgen voor betrokkene(n)?	Dit kan diverse gevolgen hebben voor de betrokkene zoals
--	--

Inschatting Impact	☐ Laag	☐ Midden	☐ Hoog
Onderbouwing:			
Kans op intreden	☐ Laag	☐ Midden	☐ Hoog
Onderbouwing:			
Risico (impact x kans)	☐ Laag	☐ Midden	☐ Hoog
Aanvullende maatregelen?	• Zorg dat de cameraman het correcte inspectieobject fotografeert. • Zorg dat de juiste invalshoeken voor de inspectiefoto's bij de cameraman bekend zijn.		
Restrisico	☐ Laag	☐ Midden	☐ Hoog
Toelichting:			

• Opslag en bewaartermijnen

Risico: De beelden en foto's worden langern bewaard dan noodzakelijk

Wat zijn de gevolgen voor betrokkene(n)?	Dit kan diverse gevolgen hebben voor de betrokkene zoals		
Inschatting Impact	☐ Laag	☐ Midden	☐ Hoog
Onderbouwing:			
Kans op intreden	☐ Laag	☐ Midden	☐ Hoog
Onderbouwing:			
Risico (impact x kans)	☐ Laag	☐ Midden	☐ Hoog
Aanvullende maatregelen?	• Zorg dat navigatiebeelden alleen zichtbaar zijn voor drone piloot, cameraman en medewerkers van de gemeente. • Zorg dat navigatiebeelden direct na de vlucht worden verwijderd. • Zorg dat bij de drone operator de gemaakte foto's alleen toegankelijk zijn voor aangewezen personen die de kwaliteitscontrole uitvoeren. • Zorg dat na overdracht van inspectiefoto's vanuit de drone operator naar de gemeente, dat die foto's bij de drone operator worden verwijderd. • Zorg dat de inspectiefoto's vanuit de drone operator rechtstreeks naar de gemeente worden verzonden.		
Restrisico	☐ Laag	☐ Midden	☐ Hoog
Toelichting:			

• Informatiebescherming

Risico: Foto's worden gelekt.

Wat zijn de gevolgen voor betrokkene(n)?	Indien foto's, verzameld door middel van drone inzet door de gemeente, op straat komen te liggen kan dit aanzienlijke schade opleveren bij burgers en het vertrouwen in de gemeente kan afnemen.		
Inschatting Impact	☐ Laag	☐ Midden	☐ Hoog
Onderbouwing:			
Kans op intreden	☐ Laag	☐ Midden	☐ Hoog
Onderbouwing:			
Risico (impact x kans)	☐ Laag	☐ Midden	☐ Hoog

Aanvullende maatregelen?	• Maak duidelijke afspraken met de drone operator op het gebied van informatiebeveiliging van de beelden, foto's en overdracht daarvan. Hierin wordt ook afgesproken dat beelden na succesvolle overdracht door de drone operator worden verwijderd. • De verbinding tussen drone camera en piloot moet zodanig beveiligd zijn, dat beelden niet door anderen toegankelijk zijn. • Indien foto's worden bewerkt door de drone operator: De opslag van te bewerken foto's bij de drone operator moet beveiligd zijn en alleen toegankelijk voor de medewerker die de kwaliteitsbewerking uitvoert		
Restrisico	☐ Laag	☐ Midden	☐ Hoog
Toelichting:			

• **Rechtmatigheid**

Risico: Er worden niet noodzakelijke persoonsgegevens verwerkt

De Piloot ziet via camera beelden om te kunnen vliegen, hier kunnen personen en persoonsgegevens (bijvoorbeeld kentekens) onbedoeld in beeld komen.

Wat zijn de gevolgen voor betrokkene(n)?	Mogelijk zijn de niet-noodzakelijke gegevens, zoals kenmerken en/of objecten te herleiden tot een individu.		
Inschatting Impact	☐ Laag	☐ Midden	☐ Hoog
Onderbouwing:			
Kans op intreden	☐ Laag	☐ Midden	☐ Hoog
Onderbouwing:			
Risico (impact x kans)	☐ Laag	☐ Midden	☐ Hoog
Aanvullende maatregelen?	• De gemeente en de drone operator hebben in onderlinge werkafspraken als uitgangspunt opgenomen dat er geen personen of irrelevante objecten worden gefotografeerd en/of anderszins worden vastgelegd. • Ongetwijfeld komt het voor dat niet noodzakelijke gegevens of personen op de foto's staan. Hierop is een kwaliteitscheck noodzakelijk waarbij niet noodzakelijke gegevens geblurd moeten worden. Deze kwaliteitscheck dient ingericht en geborgd te worden. Een mogelijkheid is dat deze activiteit door de drone operator wordt uitgevoerd, waardoor de gemeente alleen gecheckte en opgeschoonde foto's ontvangt. • Beelden blurren voordat ze gebruikt gaan worden, bij voorkeur op de camera • Geen camera, maar lidar etc. gebruiken		
Restrisico	☐ Laag	☐ Midden	☐ Hoog
Toelichting:			

Risico: Bijvangst

Wat zijn de gevolgen voor betrokkene(n)?	
--	--

Inschatting Impact	☐ Laag	☐ Midden	☐ Hoog
Onderbouwing:			
Kans op intreden	☐ Laag	☐ Midden	☐ Hoog
Onderbouwing:			
Risico (impact x kans)	☐ Laag	☐ Midden	☐ Hoog
Aanvullende maatregelen?	Werkinstructie waarin is uitgelegd hoe om te gaan met bijvangst.		
Restrisico	☐ Laag	☐ Midden	☐ Hoog
Toelichting:			

Risico: Heimelijk toezicht

Wat zijn de gevolgen voor betrokkene(n)?	<zie voor de beantwoording overweging 75 AVG>		
Inschatting Impact	☐ Laag	☐ Midden	☐ Hoog
Onderbouwing:			
Kans op intreden	☐ Laag	☐ Midden	☐ Hoog
Onderbouwing:			
Risico (impact x kans)	☐ Laag	☐ Midden	☐ Hoog
Aanvullende maatregelen?	Normale procedure volgen zoals bij “traditioneel” toezicht		
Restrisico	☐ Laag	☐ Midden	☐ Hoog
Toelichting:			

- Bijzondere persoonsgegevens**

n.v.t.

- Verwerkingsdoeleinde en doelbinding**

Risico: Inzet voor andere doeleinden (function creep)

Drones kunnen ook voor andere doeleinden worden gebruikt dan voor de inspectie ‘omdat het handig is’. Dat wordt ook wel ‘*function creep*’ genoemd. Dat zou zich bijvoorbeeld kunnen voordoen als ook andere diensten binnen de gemeente gebruik willen maken van de drone zonder dat daarbij zorgvuldige afwegingen en maatregelen zijn opgesteld.¹

Wat zijn de gevolgen voor betrokkene(n)?	De impact van <i>function creep</i> kan voor betrokkenen – afhankelijk van het doel – aanzienlijk zijn.		
Inschatting Impact	☐ Laag	☐ Midden	☐ Hoog
Onderbouwing:			
Kans op intreden	☐ Laag	☐ Midden	☐ Hoog
Onderbouwing:			
Risico (impact x kans)	☐ Laag	☐ Midden	☐ Hoog
Aanvullende maatregelen?	- Zorg dat de overdracht van foto's van de drone operator naar de gemeente door de afdeling(en) zelf wordt ontvangen en voorkom dat beeldmateriaal in een dataflow naar een andere afdeling gaat. - Eigenaarschap van de dienst: De dienst bepaalt uiteindelijk waar drones voor worden ingezet, niet de afdelingen zelf. Hierop wordt ook toezicht gehouden en aan iedere nieuwe toepassing van drones gaat een vergelijkbare risicoanalyse vooraf. Blijkt daaruit dat er een risico voor		

	betrokkenen is die niet kan worden weggenomen door middel van passende maatregelen, zie dan af van deze toepassing.		
Restrisico	☐ Laag	☐ Midden	☐ Hoog
Toelichting:			

- **Noodzaak en evenredigheid**

n.v.t.

- **Transparantie**

Risico: Datacollectie zonder dat de betrokkene geïnformeerd is.

Wat zijn de gevolgen voor betrokkene(n)?	Indien betrokkenen onvoldoende op de hoogte worden gebracht van hun betreffende persoonsgegevensverwerkingen, bestaat het risico dat inwoners niet weten welke persoonsgegevens over hen worden verwerkt en met welke partijen deze gegevens worden uitgewisseld. ¹ Hierdoor verliezen zij controle over hun persoonsgegevens en kunnen zij hun AVG-rechten niet goed meer uitoefenen, zoals correctie en inzage.		
Inschatting Impact	☐ Laag	☐ Midden	☐ Hoog
Onderbouwing:			
Kans op intreden	☐ Laag	☐ Midden	☐ Hoog
Onderbouwing:			
Risico (impact x kans)	☐ Laag	☐ Midden	☐ Hoog
Aanvullende maatregelen?	• Informeren in brieven aan de bewoners/vergunninghouders. • Informatie over het gebruik van drones voor toezicht op de website van de gemeente. • Borden voor geïnteresseerden op straat. Geef op dat bord ook aan dat het om de gemeente [naam] gaat met verwijzing naar de privacyverklaring op de website van de gemeente. • Afhankelijk van het proces is er een inspecteur/medewerker op locatie van de drone operator. Hij of zij kan burgers van informatie voorzien en hen doorverwijzen naar de juiste websitepagina.		
Restrisico	☐ Laag	☐ Midden	☐ Hoog
Toelichting:	De gemeente heeft een algemene privacyverklaring, maar daarin wordt niet beschreven hoe gegevens verwerkt (kunnen) worden door middel van drones. Daarnaast hebben betrokkenen verschillende rechten, zoals inzage, verwijdering of wijziging van hun gegevens op basis van de AVG. Als deze elementen goed gecommuniceerd worden met de betrokkenen, kan dit risico gemitigeerd worden.		

- **Rechten van betrokkenen**

Risico: Betrokkene heeft minder rechten

Wat zijn de gevolgen voor betrokkene(n)?	De betrokkene is niet goed op de hoogte hoe de AVG-rechten uitgeoefend kunnen worden.
--	---

Inschatting Impact	☐ Laag	☐ Midden	☐ Hoog
Onderbouwing:			
Kans op intreden	☐ Laag	☐ Midden	☐ Hoog
Onderbouwing:			
Risico (impact x kans)	☐ Laag	☐ Midden	☐ Hoog
Aanvullende maatregelen?	• Normale procedure volgen zoals bij “traditioneel” toezicht inclusief alle waarborgen die daarbij horen. • Zorg ervoor dat het duidelijk wordt gemaakt op welke wijze de rechten van betrokkenen kunnen worden uitgeoefend.		
Restrisico	☐ Laag	☐ Midden	☐ Hoog
Toelichting:			

- **Overig**
n.v.t.

D. Maatregelen en Restrisico's

Nr	Thema (DPIA)	Omschrijving risico (scenario)	Risico	Maatregelen	Rest risico ¹	Actiehouder	Overeengekomen realisatiedatum
1	Sturing, Toezicht en Awareness		😊		😊		
2	Betrokken partijen		😊		😊		
3	Verwerkingslocaties		😊		😊		
4	Informatiekwaliteit	Geen significante risico's vastgesteld	😊				
5	Opslagbeperking en bewaartermijnen	Geen significante risico's vastgesteld	😊				
6	Informatiebescherming		😊		😊		
7	Rechtmatigheid	Geen significante risico's vastgesteld	😊				
8	Bijzondere persoonsgegevens		😞		😊		
9	Verwerkingsdoeleinden en doelbinding		😞		😊		
10	Noodzaak en evenredigheid		😊		😊		
11	Transparantie		😞		😊		
12	Rechten van betrokkenen						
13	Overig		😞		😊		

Legend



Hoog



Middel



Laag

¹ Wanneer het restrisico hoog is, moet voorafgaand aan de verwerking de Autoriteit Persoonsgegevens geraadpleegd worden. Het ECP adviseert hierbij.

Akkoordverklaring Proceseigen(a)r(en)/gemandateerde(n)

Ik ben akkoord met de bevindingen van deze DPIA en draag zorg voor tijdige uitvoering van de maatregelen.

Toelichting: Het akkoord wordt u per mail gevraagd. U kunt ook gedeeltelijk akkoord gaan of akkoord gaan onder voorwaarden. Dit moet dan wel deugdelijk gemotiveerd worden. De mail met uw akkoordverklaring wordt in de finale versie van deze DPIA als Outlook-bestand in deze bladzijde opgenomen.

Advies Functionaris Gegevensbescherming (FG)

Toelichting: Het advies wordt per mail aan de privacy coördinator verstrekt. De mail met het advies van de FG wordt in de finale versie van deze DPIA als Outlook-bestand bestand in deze bladzijde opgenomen.