Onderwerp
Privacy GEB
UAV politie

Organisatieonderdeel
t.b.v. Stuurgroep UAV

Behandeld door
10.2.e

Functie
Projectmanager

Telefoon
10.2.e

E-mail
10.2.e @politie.nl

Ons kenmerk

Uw kenmerk

In afschrift aan

Datum
2 maart 2020

Bijlage(n)
0

Inleiding

Bij privacy gaat het over het beschermen van iemands persoonlijke levenssfeer.

Een UAV (Unmanned Aerial Vehicle, 'drone') kan niet alleen foto's of videobeelden maken en versturen, maar kan ook, afhankelijk van de technologie waarmee de UAV is uitgerust, communicatiesignalen afluisteren, gezichten opsporen, objecten en personen opsporen en identificeren, hun bewegingen opnemen of gedrag signaleren dat als abnormaal worden beschouwd, etc.

Het is niet vreemd dat er zorgen zijn over privacy als UAVs worden ingezet voor politietaken. Vanwege deze en andere risico's heeft de Korpschef in 2013 besloten dat "*alle UAV-operaties door de politie worden stopgezet tot een visie en inzetcriteria voor de inzet van UAV's door de politie zijn uitgewerkt.*"

In deze memo wordt kort toegelicht hoe sinds 2013 is omgegaan met privacy in relatie tot UAV inzet. Vervolgens worden ook 3 scenario's genoemd hoe in de toekomst met privacy omgegaan kan worden.

Privacy in relatie tot UAV inzet politie

In 2014 is het visiedocument Contourennota Onbemande Luchtvaartuigen opgesteld. In dit document is privacy nadrukkelijk meegenomen. In dit document staat o.a.:

"*Hoewel met de huidige inzet van onbemande luchtvaartuigen (Raven) ten behoeve van de politie op dit moment nauwelijks gezichtsherkenning mogelijk is, is dit in de toekomst wel mogelijk. Hierdoor zullen privacyaspecten een steeds nadrukkelijker rol in de afweging tot inzet gaan spelen. Het inzetten van onbemande luchtvaartuigen dient derhalve steeds te worden getoetst aan proportionaliteit en subsidiariteit*."

Inmiddels zijn we 6 jaar verder en hebben we 7 operationele UAV-proeftuinen en zijn 4 UAV-proeftuinen in de opstartfase. Per proeftuin wordt gekeken naar opbrengsten, kosten en risico's. Privacy wordt daarin nadrukkelijk meegenomen en voor alle duidelijkheid: gezichtsherkenning wordt bewust nog niet toegepast in combinatie met UAV, terwijl dit technisch eenvoudig realiseerbaar is.

Samengevat kan gesteld worden dat zeer beperkt UAV-gegevens worden opgeslagen: dit wordt zeker niet centraal, op grote schaal, doorzoekbaar etc. gedaan. In de meeste gevallen worden zorgvuldig beelden verzameld die vervolgens formeel worden overgedragen aan de opdrachtgever. De opdrachtgever is vervolgens verantwoordelijk voor verwerking van de gegevens conform WPG en andere wet- en regelgeving. Vanuit het project Onbemande Luchtvaartuigen (2015 t/m 2017) en het vervolgproject UAV (2018 t/m 2020) wordt voldaan aan alle wet- en regelgeving.

Inzetbeleid en GEB

Medio 2018 is het Inzetbeleid UAV opgesteld en daarna heeft dit Inzetbeleid UAV het reguliere besluitvormingsproces doorlopen. Medio 2019 heeft de COR een positief advies uitgebracht t.a.v. het Inzetbeleid UAV en daarna is het formeel vastgesteld

Gekoppeld aan het positief advies heeft de COR gesteld dat "*er een inzetkader, handelingskader en GEB worden opgesteld*". Een GEB is een 'Gegevensbeschermingseffectbeoordeling', met als doel privacyrisico's van de gegevensverwerking vooraf in kaart brengen en beheersmaatregelen bepalen om de risico's te verkleinen.

Vanuit het project is herhaaldelijk contact geweest met Privacyfunctionarissen over een GEB voor UAV. Vanuit 10.2.e (Privacyfunctionaris LE) is gesteld: "*We kunnen onderzoeken of voor de verwerking UAV überhaupt een GEB noodzakelijk is. Hiervoor is de Checklist Pre-GEB bijgesloten.*" en "*De Checklist Pre-GEB bevat een negental criteria. Als de verwerking Unmanned Aerial Vehicles voldoet aan twee of meer van de genoemde criteria is er sprake van een hoog risico en dient er daadwerkelijk een gegevensbeschermingseffectbeoordeling te worden uitgevoerd*."

De uitslag van de pre-GEB voor de negen criteria is als volgt:

1. Het beoordelen van mensen op basis van persoonskenmerken: **N.V.T.**
2. Geautomatiseerde beslissingen: **N.V.T.**
3. Stelselmatige en grootschalige monitoring: **N.V.T.*)**
4. Het verwerken van gevoelige gegevens, inclusief zeer persoonlijke gegevens **N.V.T.**
5. Grootschalige gegevensverwerkingen **N.V.T.**
6. Koppelen en combineren van politiegegevens **N.V.T.**
7. Het verwerken van gegevens over kwetsbare personen **N.V.T.**
8. Het gebruik maken van nieuwe technologieën **N.V.T.**)**
9. Verwerkingen die leiden tot de blokkering van een recht, dienst of contract. **N.V.T.**

*) Soms worden in het kader van OOV beelden gemaakt en doorgestuurd naar de meldkamer. Dat kan zijn in het kader van een protestacties, demonstraties of een festival (crowd control), maar is altijd tijdelijk en niet stelselmatig en zeker niet grootschalig. (Dit zou ook vergelijkbaar kunnen worden gedaan door een politiehelikopter)

**) Uiteraard is UAV / drones een relatief nieuwe technologie. De wijze waarop dit tot nu toe wordt gebruikt door politie is relatief traditioneel. Het gaat dan om maken van overzichtsfoto's die eventueel met een helikopter gemaakt zouden kunnen worden. Innovatieve technieken als AI worden bewust nog niet toegepast. De in de checklist genoemde technologieën zoals gezichts- of spraakherkenning en 'the internet of things' zijn van een totaal andere (en veel ingrijpendere) orde.

N.a.v. deze uitslag heeft 10.2.e (Privacyfunctionaris LE) gesteld:

"*Als ik jouw antwoorden lees zie ik geen reden tot het uitvoeren van een GEB. Op geen enkel criterium wordt er gescoord.*

Ten aanzien van jouw opmerkingen; deze zijn verhelderend. Monitoring moet met name stelselmatig en grootschalig zijn. We spreken over nieuwe technologieën voor bijvoorbeeld identificatie, in dit geval niet over de technologie van de drone an sich.

Dit alles overziend zie ik geen verwerking die gelet op de aard, de omvang, de context of doelen ervan, waarschijnlijk een hoog risico voor de privacy van de betrokkene oplevert. 11.1

Scenario's vervolg

1. Geen GEB, gegeven uitslag pre-GEB
2. Wel GEB, ondanks uitslag pre-GEB
3. Aanvullende acties zoals communicatie.

Toelichting Scenario 1. Geen GEB, gegeven uitslag pre-GEB
De Privacyfunctionaris verwacht – gegeven de uitkomst van de pre-GEB – dat een GEB weinig oplevert, terwijl dit wel veel werk kost.

Een optie is om opdrachtgevers van UAV-inzetten te wijzen op de pre-GEB.

Toelichting Scenario 2. Wel GEB, ondanks uitslag pre-GEB
Een reden voor het uitvoeren van een GEB is dat dit is toegezegd aan de COR, gekoppeld aan het Inzetbeleid UAV.

Als wel een GEB wordt uitgevoerd, is de vraag 11.1 .

Toelichting Scenario 3. Aanvullende acties zoals communicatie.
Veel zorgen over privacy en inzet van UAV hebben te maken met misverstanden. Misverstanden kunnen weggenomen worden via communicatie. Bij communicatie is het van belang onderscheid te maken tussen de volgende stakeholders:

- Intern project UAV (inclusief Proeftuinen)
- Opdrachtgevers (intern politie)
- Extern politie (burgers, journalisten, belangenorganisatie e.d.)

11.1 . Ook de afspraak dat een wijziging waardoor 1 of meer criteria van de pre-GEB wel van toepassingen worden eerst aan de Stuurgroep UAV voorgelegd moeten worden

Bij communicatie extern politie (burgers, journalisten, belangenorganisatie e.d.) kan gedacht worden aan communicatie via www.politie.nl

Gevraagd besluit en aanbeveling
Aan de Stuurgroep UAV wordt gevraagd om een besluit te nemen over het wel/niet uitvoeren van een GEB.

11.1