

Bijlage 5: DPIA

5.1 Vragenlijst DPIA ten behoeve van inzet (helm)camera's door de brandweer ter bescherming van medewerkers en materieel bij (mogelijke) ongeregelde heden

Aangezien een DPIA (mogelijk) noodzakelijk is dienen de volgende vragen beantwoord te worden.

Zijn er (externe) partijen betrokken bij deze verwerking? Zo ja, welke?	Nee
Welke rol hebben deze externe partijen bij de verwerking? <i>Verwerken deze externe partijen bijv. persoonsgegevens in opdracht van de VRGZ?</i>	Geen
Worden de gegevens buiten de organisatie opgeslagen of gebruikt? Zo ja, waar? <i>Denk aan systemen/applicaties waar persoonsgegevens verwerkt worden.</i>	Nee, de beelden zijn enkel lokaal te bekijken op het apparaat (geheugen), de SD-kaart ed. die via een computer wordt ontsloten. Bij een download wordt dit opgeslagen in het netwerk van de VRGZ bereikbaar met login van de apparaat beheerder die opdracht heeft gekregen de data van het apparaat te halen. Op een aantal apparaten kan live beeld meegekeken worden.
Worden de persoonsgegevens buiten Nederland gebruikt (denk hierbij aan cloudapplicaties, datacenters, tussenpersonen, etc.)?	Nee
Zijn er bewaartermijnen vastgesteld? <i>Hiervoor kun je navraag doen bij Informatiebeheer</i>	Ja, binnen de VRGZ worden beelden maximaal 14 dagen bewaard.
Is de Security Officer al betrokken?	Ja, vanaf het opslaan van de beelden op het VRGZ netwerk valt dit onder de reguliere verwerking van gegevens.
Waar worden de gegevens verkregen? <i>Komen de gegevens van de betrokkene zelf of komen ze uit een applicatie? Het kan ook zijn dat ze van een andere organisatie komen.</i>	Door betrokkenen te filmen met een helmcamera in de openbare ruimte of in een besloten ruimte (die betreden wordt onder de voorwaarden die daarvoor gelden op grond van de wet)
Welke persoonsgegevens worden verwerkt? <i>Geef aan welke gegevens worden verwerkt in de gegevensverzameling.</i>	Camerabeelden van burgers en medewerkers
Is een verwerkersovereenkomst nodig of aanwezig? <i>Geef aan of een verwerkersovereenkomst nodig is of eventueel al is afgesloten. Een verwerkersovereenkomst sluit je af met derden die namens jouw persoonsgegevens verwerken</i>	Nee, omdat er geen externe partijen betrokken zijn. Camerabeelden bekijken wordt enkel uitgevoerd door geautoriseerde medewerkers brandweer Gelderland-Zuid. Aandacht wordt gevraagd voor het geval defecte apparaten naar de leverancier teruggaan voor reparatie en waarop nog beelden staan.

5.2 Data Protection Impact Assessment (DPIA)

Organisatiegegevens

Naam, adres van organisatie: Veiligheidsregio Gelderland – Zuid, Professor Bellefroidstraat 11, 6525 AG NIJMEGEN

Opsteller DPIA: Marcel Jonkman (Projectleider team Beleid & ondersteuning brandweer / VRGZ)

Naam en contactgegevens FG : Team Informatiemanagement VRGZ.

- a. Gosse Bijlenga (Functionaris gegevensbescherming)
gosse.bijlenga@vrgz.nl.
- b. Barbara Dauwerse (Privacy Officer)
Barbara.dauwerse@vrgz.nl
- c. Heleen Verdonck (Adviseur Informatie veiligheid)
heleen.verdonck@vrgz.nl. [+31651214853](tel:+31651214853)

Overige betrokkenen en geraadpleegde experts:

Mr. Marieke Thijssen

Hekkelman Advocaten N.V.

m.thijssen@hekkelman.nl

024 - 382 83 88

Gegevens van de verwerking

Beschrijf hier om welke persoonsgegevens het gaat (naam, email, medisch, ...).

Het betreft camerabeelden van burgers en medewerkers.

Met welk doel en in welk proces worden deze gegevens gebruikt?

Voor het beschermen van medewerkers en materieel bij (mogelijke) ongeregelde heden.

De noodzaak van het cameragebruik is dan zowel preventief als repressief. Het preventieve effect wordt vooral bereikt doordat potentiële kwaadwillenden zich bewust zijn van het filmen, waardoor agressie en geweld en andere strafbare feiten tegen medewerkers mogelijk voorkomen kunnen worden.

Het repressieve effect ontstaat omdat achteraf zo nodig gekeken kan worden wie strafbare feiten heeft veroorzaakt. Denk aan diefstal van kostbare materialen of strafbaar gedrag in crisissituaties tegen hulpverleners.

Welke groepen betrokkenen zijn de persoonsgegevens van opgenomen:

Burgers en medewerkers.

Is deze DPIA voor een bestaande situatie, of voor een nieuw voorgestelde situatie?

Deze DPIA wordt uitgevoerd voor een bestaande situatie.

Moet een DPIA worden uitgevoerd

Een DPIA is alleen verplicht als een gegevensverwerking waarschijnlijk een hoog privacy risico oplevert voor de betrokkenen (de mensen van wie de organisatie gegevens verwerkt). Dat is in ieder geval zo als een organisatie:

1. op grote schaal bijzondere persoonsgegevens verwerkt;
2. op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied (bijvoorbeeld met cameratoezicht).

Om te bepalen of er mogelijk sprake is van een hoog risico hanteren de toezichthouders de onderstaande vuistregel. Er is sprake van een hoog risico men aan twee of meer van de onderstaande negen criteria voldoet:

1. evaluatie van personen of scoretoekenning;
2. geautomatiseerde besluitvorming met rechtsgevolg of vergelijkbaar wezenlijk gevolg;
3. stelselmatige monitoring;
4. gevoelige gegevens of gegevens van zeer persoonlijke aard;
5. op grote schaal verwerkte gegevens;
6. matching of samenvoeging van datasets;
7. gegevens met betrekking tot kwetsbare betrokkenen;
8. innovatieve toepassing van nieuwe technologische of organisatorische oplossing;
9. blokkering van een recht, dienst of contract.

Aan welke criteria voldoet deze verwerking? Geef voor elk criteria een korte motivatie

Door de inzet van helmcamera's door de brandweer is er sprake van criterianummer 4 en 8 uit de laatste opsomming.

Beschrijf hier in meer detail hoe de gegevensverwerking gaat.

Het betreft incidenteel cameratoezicht waarbij camerabeelden kunnen worden bewaard. Het gebruik is vooraf door de korpsleiding (BMT, teamleiders IB, teamleiders Vakbekwaamheid of de HOvD) bepaald. Zie verder paragraaf 2.2 onder 2, hoofdstuk 3 en met name paragraaf 4.3 van het concept-camerabeleid.

Hoe / waar wordt de informatie verzameld?

Door een helmcamera die gekoppeld wordt aan een computer worden beelden ontsloten naar het VRGZ ICT netwerk en in een bestandsmap van de Apparaat beheerder geplaatst.

Waar wordt deze opgeslagen? Wie kan hier bij?

De beelden zijn toegankelijk via een computer welke in het VRGZ netwerk is aangesloten. Download van beelden van het apparaat gebeurt in een map in de VRGZ omgeving waar de Apparaat beheerder toegang tot heeft. De beelden mogen enkel in overeenstemming met het concept-camerabeleid en in het bijzijn van de apparaat beheerder worden bekeken door medewerkers die hier toestemming voor hebben van degene die beslist over de inzet van de helmcamera's.

Hoe wordt de informatie gebruikt? Wordt elk veld gebruikt?

Alleen als dat (mogelijk) nodig is voor evaluatie of aangifte of op vordering van de officier van justitie worden de camerabeelden overgezet op het VRGZ-netwerk en (kortdurend) bewaard.

Wat zijn de doelen van de verwerking? Kunnen deze doelen ook zonder de gegevens worden behaald?
Zie hiervoor bij doel.

Wordt binnen het proces om toestemming gevraagd? Zijn er latere uitschrijf/opt-out-mogelijkheden?
Ja, aan de medewerker die de helmcamera gaat dragen wordt toestemming gevraagd.

Wat is de bewaartermijn van de gegevens? Hoe is de verwijdering van de gegevens geregeld?
De bewaartermijn van de gegevens is maximaal 14 dagen.

Welke hardware en software wordt gebruikt bij de gegevensverwerking?
Camera's, computers met software waarmee de beelden worden opgeslagen en bekeken kunnen worden. Hiervoor is geen software nodig. Het gaat om beeldbestanden die met een mediaplayer bekeken kunnen worden.

Welke afdelingen, leveranciers en andere partijen zijn als verwerker bij de verwerking betrokken?
De medewerker van de afdeling Incidenten bestrijding van de sector brandweer die belast met het apparaat beheer. Er zijn geen externe verwerkers.

Is er sprake van internationale doorgifte? Welke landen betreft dit?
Nee.

Waar wordt de data gearchiveerd? Is dit papier of digitaal?
Geen archivering.

Wat is de verwachte omvang van de gegevensverwerking (aantallen betrokkenen)
Het gebruik van de camera's wordt toegepast ingeval van mogelijke ongeregelde heden. Of daar (mogelijk) sprake van is wordt vooraf door de korpsleiding (directie VRGZ, BMT, teamleider IB of HOvD) bepaald. Dit kan een type situatie zijn, een moment in het jaar of een bepaald gebied waar zich het risico voordoet. Afhankelijk daarvan is het aantal betrokkenen de ene keer groter dan de andere keer. Vooralsnog zijn de helmcamera's alleen ingezet tijdens de Jaarwisseling. Er kunnen circa 50 cameras tegelijk ingezet worden.

In het kader van de proportionaliteit wordt door de beslisser aangegeven wie, wanneer en waar de camera aangezet moet worden.

Beoordeling noodzaak en proportionaliteit

Is er sprake van een duidelijk gespecificeerd doel? Wat is dit doel precies, en waarom is dit legitiem?
Verwezen wordt naar het camerabeleid waarin alles is uitgewerkt.

Ja, de helmcamera's worden alleen kortdurend ingezet bij mogelijke ongeregelde heden waarbij medewerkers mogelijk bescherming nodig hebben zodat zij hun werk kunnen doen. Of sprake kan zijn van dergelijke ongeregelde heden, wordt door de korpsleiding bepaald op basis van ervaring. Alleen als de ervaring leert dat bij een bepaalde situatie of op een bepaald moment of in een bepaald gebied ongeregelde heden te verwachten zijn, waarbij medewerkers mogelijk bescherming nodig hebben, dan worden de helmcamera's ingezet. Tot dusver is dat alleen het geval bij de jaarwisseling.

Kan dit doel ook zonder deze persoonsgegevens worden behaald? Waarom niet, of waarom doet u het niet anders?

Nee, in de hotzone (gevaarlijk gebied) van een crisis is werken alleen voor de brandweer mogelijk inzet van andere personen om de brandweer te beschermen is niet mogelijk. Verder wordt gewerkt onder grote tijdsdruk.

Ja, door middel van surveillance/bewaking door de politie. Dit is echter niet altijd mogelijk, in verhouding kostbaarder en kan tevens als inbreuk op privacy worden ervaren met kans op extra escalatie.

Is er sprake van een duidelijke maximale bewaartermijn?

Ja, zie hiervoor.

Wordt er voldoende informatie verstrekt aan betrokkene? Is het voor betrokkenen duidelijk welke rechten zij hebben en hoe zij deze kunnen uitoefenen?

Verwezen wordt naar het camerabeleid waarin alles is uitgewerkt.

- Medewerkers VRGZ worden geïnformeerd over het Cameragebruik door de brandweer VRGZ.
- Externen die in beeld zijn gekomen worden als de tijd dit toelaat vooraf of achteraf geïnformeerd.

Hoe is het recht op inzage gewaarborgd?

De betrokkene kan een verzoek bij de VRGZ doen. Zie verder het camera beleid.

Hoe is het recht op rectificatie gewaarborgd?

Dit is niet mogelijk bij camerabeelden.

Hoe is het recht op verwijdering gewaarborgd?

Verwijdering is mogelijk als de betrokkene daar op goede gronden om verzoekt (maar de beelden worden zeer kort bewaard, dus de kans op een verzoek om rectificatie is klein).

Hoe is het recht op overdraagbaarheid van gegevens gewaarborgd?

Dit is gelet op de grondslag van de verwerking (artikel 6 lid 1 onder f AVG) alleen aan de orde als de medewerker daar om verzoekt.

Beoordeling van de privacyrisico's

Hoe schat u de kans en impact van de volgende risico's:

Risico	Hoe kan dit risico zich voordoen?	Kans dat dit in een jaar gebeurt	Impact op betrokkenen
Onrechtmatige toegang – interne medewerkers	Wanneer een medewerker (inbreekt) de inlog code kraakt of inlogcode van geautoriseerde medewerker krijgt of steelt	Medium	Medium, de beelden van betrokkenen kunnen bekeken worden. De aanwezigheid van betrokkene op die locatie wordt bekend aan medewerker.
Onrechtmatige toegang – door buitenstaanders	Wanneer iemand inbreekt en inlog code kraakt	Laag	Medium, de beelden van betrokkenen kunnen bekeken worden. De aanwezigheid van betrokkene op die locatie wordt bekend aan buitenstaander
Ongewenste wijziging van gegevens – interne medewerkers	n.v.t.		
Ongewenste wijziging van gegevens – door buitenstaanders	n.v.t.		
Verlies van een helm en/of camera	De camera zit met een houder vast aan de helm. Bij stoten zou deze kunnen afbreken. De maker van de beelden kan de helm afzetten en ergens laten liggen.	Zeer laag	Zoek raken van de camera met daarop beelden. Eventuele Kwaadwillenden die de camera en of helm vinden kunnen met de beelden aan de haal gaan. Dit beschouwen als een datalek.
Verdwijnen / zoekraken van gegevens	n.v.t.		Dit is een datalek. De FG, privacy officer en CISCO worden geïnformeerd over het verlies van de gegevens en er wordt melding gemaakt bij AP (voorheen CBP)

Maatregelen

Kunt u per risico aangeven welke maatregelen u neemt om de gegevens te beschermen:

De beelden zijn enkel toegankelijk via de beheerder van het apparaat.

Bij verlies of verdwijnen van beeldmateriaal zal na constatering melding bij de teamleider IB worden gedaan waarop deze een intern onderzoek zal starten en aangifte worden gedaan bij de politie en melding bij de **AP** Autoriteit Persoonsgegevens (voorheen CBP) van de verdwijning van beeldmateriaal. Indien bekend is welke personen op de beelden staan zullen zij worden geïnformeerd over het verlies van de gegevens. Vervolgens zal de casus worden geëvalueerd om herhaling te voorkomen.

Zijn er nog aanvullende organisatorische maatregelen die u neemt?

De werkwijze is vastgelegd in een beleid.

Zijn er nog aanvullende technische maatregelen die u neemt?

De beelden worden na 4 weken verwijderd door de apparaat beheerder.

Is het duidelijk wie na afloop van het project verantwoordelijk is voor het in stand houden en evalueren van de getroffen maatregelen?

Ja, de teamleider Incidentenbestrijding (IB) is verantwoordelijk voor het beheer van de camera apparaten vastgelegd in het camerabeleid brandweer VRGZ.

Advies van de FG

Naam FG: Gosse Bijlenga

Datum van advies: 27 november 2024

Antwoorden van FG:

Als FG heb ik de documenten beoordeeld. De huidige documenten zijn in de goede richting, maar nog onvoldoende om vast te stellen. De jaarwisseling 2024 kan voor nu als pilot dienen om verdere ervaring op te doen met dit aangescherpte beleid en tzt in Q1 2025 door te ontwikkelen.

Zijn de gegevensverwerking en doeleinden duidelijk omschreven?

Ja

Is de verwerking van de persoonsgegevens noodzakelijk of proportioneel voor de doeleinden?

Ja

Zijn de privacy risico's voldoende in kaart gebracht? Welke risico's ontbreken nog?

Ja

Advies van betrokkenen en vertegenwoordigers

Is er voor deze DPIA gesproken met betrokkenen of vertegenwoordigers?

De OR medezeggenschap zal worden geïnformeerd.

Voorafgaande raadpleging

Komt er uit de DPIA dat de verwerking een hoog risico oplevert als u geen risicobeperkende maatregelen neemt? Geef antwoord en motivatie hieronder:

Nee, de risico's zijn medium tot laag te noemen. Er zijn voldoende risicobeperkende maatregelen genomen.