

Gegevensbeschermings- effectbeoordeling

*Uitwerking artikel 35 van de Algemene verordening
gegevensbescherming EU 679/2016*

**Gemeente Utrecht / Vergunningen, Toezicht
en Handhaving / Toezicht en Handhaving
Openbare Ruimte**

Bodycam

Datum: 15-06-2020
Projectnummer: nvt
Projectleider: Nvt
Opdrachtgever: Arie Godee / Hans Lesscher
Versie: 1.0
Opstellers: Sahar Altaee
Functie: Beleidsadviseur
Validatie door: René van der Stel
Functie: DISO

Versiebeheer

Versies

Versie	Datum	Auteur	Samenvatting van de wijzigingen
0.1	23-04-2020	Sahar Altaee	Concept ter bespreking met DISO
1.0	28-04-2020	Sahar Altaee	Concept ter bespreking privacysprekkuur
1.0	14-05-2020	Sahar Altaee	Concept ter bespreking met FG
1.0	9-6-2020	Sahar Altaee	Definitieve versie voorgelegd aan FG en CISO
1.0	15-5-2020	Sahar Altaee	Definitieve versie ter ondertekening

Advies CISO

Versie	Datum	CISO	Advies
1.0	5-5-2020	Mark van Vliet	Op beveiligingsgebied heb ik de volgende vragen: 1. De keten van versleuteling is mij niet helemaal duidelijk. 2. Het is me niet helemaal duidelijk hoe toegang tot de beelden is geregeld. 3. Met betrekking tot de logging is eea onduidelijk. 4. Met betrekking tot de privacy software: a. Op welk moment in het proces wordt deze software toegepast? Is dit op de camera zelf of is dit post production op de server? b. Is het blurren omkeerbaar? (ik neem aan dat mensen die voor problemen zorgen geïdentificeerd moeten kunnen worden?) 5. Is er een BIA/risico analyse uitgevoerd en zijn er op basis hiervan passende maatregelen genomen? 9-6-2020 Sahar Altaee: De CISO heeft gevraagd om een uitgebreidere uitwerking op informatiebeveiliging. Dit is verwerkt in onderdeel 8 en 16. De leverancier kan voldoen aan de eisen van de gemeente op het gebied van informatiebeveiliging.
1.0	14-5-2020	Mark van Vliet	Leverancier laat in haar antwoorden op de gestelde vragen zien serieus nagedacht te hebben over de beveiliging van de (gegevens op de) bodycams. Echter leverancier beschikt niet over adequate documentatie waarin de werking van deze beveiliging op een

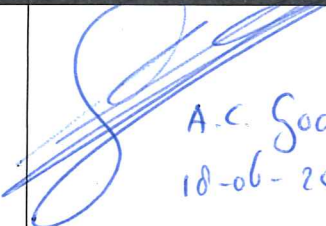
			heldere manier is opgenomen. Dit zorgt ervoor dat toetsing van deze beveiliging slechts in beperkte mate kan plaatsvinden en maakt het lastig voor de gemeente om aan te tonen dat ze passende maatregelen conform artikel 32 hebben genomen. Wat mij betreft is het ontbreken van dergelijke documentatie een risico dat in de pia opgenomen zou moeten worden. Dit risico ziet concreet op testbaarheid en aantoonbaarheid van passende maatregelen. Ik zou voorstellen dat met de leverancier afspraken worden gemaakt over het opstellen van passende documentatie. Indien die afspraken op hoofdlijnen akkoord zijn zou dit een verdere uitrol van de pilot fase naar mijn mening niet in de weg hoeven te zitten. 15-6-2020 Sahar Altaee: Dit is als risico toegevoegd bij onderdeel 18. Bij onderdeel 19 zijn de te nemen maatregelen beschreven.
--	--	--	---

Bindend advies FG

Versie	Datum	FG	Advies
	15-5-2020	Hans van Impelen	Het inzetten van camera's in de publieke ruimte ligt maatschappelijk en politiek gevoelig. In het coalitieakkoord is vastgelegd dat bij verwerken van persoonsgegevens een ethisch assessment wordt uitgevoerd. 1. Advies: voer voor deze verwerking een ethisch assessment uit (bijv. door middel van de DEDA methode van de Utrecht Dataschool van de Universiteit Utrecht) waarbij voldoende verschillende belanghebbenden (of vertegenwoordigers van belangengroepen) worden betrokken. (Bij het intern uitgevoerde ethisch assessment zijn geen extern belanghebbenden betrokken. 20-5-2020, Sahar Altaee: Na overleg met Donovan Karamat Ali is aangegeven dat een ethisch assessment met externe deelnemers op dit moment geen vereiste is voor de DPIA. Wel heeft er een intern ethisch assessment plaatsgevonden over dit vraagstuk. 2. Op grond van artikel 27 van de Wet op de ondernemingsraden is toestemming van de

			ondernemingsraad vereist. Advies: toon aan dat voorafgaand aan de invoering van de bodycams de vereiste toestemming van de ondernemingsraad is verkregen. 9-6-2020, Sahar Altaee: Instemming van OR is op 28-5-2020 verkregen. 3. De inzet van camera's ligt politiek gevoelig. De focus van VTH is in het "Handhavingsprogramma 2020-2023" gecommuniceerd. Hierin is geen voornemen voor de inzet van bodycams opgenomen. Advies: informeer de gemeenteraad voorafgaand aan de invoering van de bodycams. 20-5-2020, Sahar Altaee: Na positief besluit van het college om de bodycam in te voeren, zal de raad geïnformeerd worden.
--	--	--	--

Goedkeuring

Versie	Datum	Naam	Ondertekening
1.0		Arie Godee / Hans Lesscher Vergunningen Toezicht en Handhaving	 A.C. Godee 10-06-2020

Voorbereiding: Beschrijving kenmerken gegevensverwerkingen

Beschrijf op gestructureerde wijze de voorgenomen gegevensverwerkingen, de verwerkingsdoeleinden en de belangen bij de gegevensverwerkingen.

1. Voorstel

Beschrijf het voorstel waar de gegevensbeschermingseffectbeoordeling op ziet en de context waarbinnen deze plaatsvindt op hoofdlijnen.

Deze DPIA gaat in op het gebruik van bodycams door de aangewezen toezichthouders en buitengewoon opsporingsambtenaren van VTH, (hierna te noemen: Handhavers VTH). De DPIA beantwoordt de vraag of de risico's ten aanzien van de rechten en vrijheden van de betrokkene acceptabel zijn.

Kort wordt eerst de context van de werkzaamheden geschetst alvorens in wordt gegaan op de aanleiding om bodycams in te gaan zetten.

VTH heeft toezichthouders en boa's in dienst. Zij hebben als taak het handhaven en toezichthouden op geldende wet- en regelgeving. Dit betreft zowel landelijke als lokale regelgeving. De juridische grondslag voor toezichthouders en hun kaders waar binnen zij mogen werken staan beschreven in de AwB. De term toezichthouder is gedefinieerd in artikel 5:11 AwB. Zij houden alleen toezicht op de wet- en regelgeving waarvoor zij zijn aangewezen.

VTH heeft ook boa's, of handhavers, in dienst. Boa's vinden hun wettelijke grondslag in artikel 142 Sv. Zij hebben strafrechtelijk opsporingsbevoegdheid en mogen binnen het domein waarin zij zijn aangesteld strafbare feiten opsporen. Een toezichthouder kan tevens opsporingsambtenaar zijn.

Handhavers VTH zijn aangewezen om toezicht te houden en te handhaven op aangewezen wet en regelgeving. Hieronder een niet limitatieve lijst van wet- en regelgeving waarop Handhavers VTH mogen handhaven. Hiermee wordt de grondslag en onderbouwing van het optreden van Handhavers VTH van de meest voorkomende werkzaamheden en werklocaties onderbouwd. De uitvoering van toezicht en handhaving zijn een publiek rechtelijke taak, waarover het College of de gemeenteraad beslist.

- APV: Algemene Plaatselijke Verordening van Utrecht
- DHW: Drank- en Horecawet
- WWV: Wegenverkeerswet 1994
- RVV: Reglement verkeersregels en verkeerstekens 1990
- WM: Wet Milieubeheer
- Wp2000: Wet Personenvervoer 2000
- HWV: Huisvestingswet 2014
- Artikel 225 Gemeentewet (Parkeerbelasting)
- Wegsleepverordening
- Afvalstoffenverordening Utrecht
- Wet administratiefrechtelijke handhaving verkeersvoorschriften
- Artikel 142 Wetboek van Strafvordering
- Regelingsdomeinlijsten Buitengewoon opsporingsambtenaar

Bodycam als persoonlijk beschermingsmiddel

Werknemers moeten veilig en gezond kunnen werken. In de Arbowet staan de kaders en verplichtingen van werkgevers om Arbobeleid te voeren. De bodycam wordt aan de Handhavers VTH ter beschikking gesteld als maatregel om te voldoen aan de verplichting zoals is vastgesteld in artikel 3 lid 1 onder b Arbeidsomstandighedenwet. De bodycam wordt ingezet als persoonlijk beschermingsmiddel. De bodycams zullen niet worden gebruikt voor cameratoezicht in het kader van openbare orde. Met de inzet van bodycams wordt gepoogd om incidenten en onrechtmatige

gedragingen jegens de Handhavers VTH te voorkomen en hiermee de veiligheid van de Handhavers VTH te garanderen en psychosociale arbeidsbelasting zoveel mogelijk te beperken. De Handhavers VTH dragen de bodycams tijdens werkzaamheden in het kader van de handhaving van de lokale veiligheid en leefbaarheid, een publiekrechtelijke taak van de gemeente. De Handhaver VTH zet de bodycam enkel aan als de situatie op straat er om vraagt hun persoonlijke veiligheid te beschermen.

Pilot

Middels een pilot van een half jaar zetten we 24 bodycams in bij Handhavers VTH. De Handhavers VTH kunnen tijdens de diensten in de pilot periode gebruik maken van de 6 bodycams per dienst en per duo wordt 1 bodycam meegenomen. Er zijn per etmaal 3 diensten. Na de pilot zal uit de evaluatie moeten blijken of de bodycams hebben bijgedragen aan het veiligheidsgevoel van Handhavers VTH en of het gewenste de-escalerende effect werd bereikt. Naar aanleiding van de evaluatie wordt bepaalt of bodycams definitief ingevoerd gaan worden.

2. Persoonsgegevens

Som alle categorieën van persoonsgegevens op die worden verwerkt. Geef per categorie van betrokkene aan welke persoonsgegevens van hen verwerkt worden. Deel deze persoonsgegevens in onder de typen: gewoon, bijzonder, strafrechtelijk en wettelijk identificatienummer. Maak gebruik van het bijgevoegde overzicht van soorten persoonsgegevens.

Beeldmateriaal – bijzondere persoonsgegevens

Geluid – bijzondere persoonsgegevens

3. Gegevensverwerkingen

Geef alle voorgenomen gegevensverwerkingen weer.

Opname

De handhavers van VTH worden geïnstrueerd over wanneer en hoe hij de bodycam mag en moet gebruiken in overeenstemming met het bejegeningprotocol. Als een situatie dreigt te escaleren of is geëscaleerd kan de handhaver VTH kiezen om de bodycam te activeren. Daarbij geeft hij indien mogelijk eerst een mondelinge waarschuwing en start pas daarna de opname, als hij dit niet vooraf kan zeggen dan meldt hij dat hij de opname heeft gestart. De bodycam staat continu stand-by en maakt opnames. Wanneer de opnameknop wordt ingedrukt, worden de voorafgaande 120 seconden ook vastgelegd waarmee ook de aanleiding van het incident is vastgelegd. Dat heet pre-recording. Als de bodycam niet wordt geactiveerd zal hij de twee minuten steeds overschrijven en worden deze opnames niet bewaard. Bij evaluatie van de pilot zal blijken of de ingestelde pre-recording van 120 seconden voldoende of te veel is om de aanleiding te kunnen vastleggen. De opname wordt direct uitgezet, nadat de dreigende situatie voorbij is of er geen sprake is van escalatie. De bodycam wordt dan weer in de stand-by stand gezet. Bovenstaande zorgt ervoor dat de inbreuk op de privacy beperkt blijft. Beelden worden alleen vastgelegd in het geval van een dreigende, escalerende situatie.

Overdracht van bodycam naar dockingstation naar systeem op computer

De beelden worden versleuteld op de bodycam opgeslagen en kunnen niet ter plekke worden bekeken en/of verwijderd worden. Na de dienst wordt de bodycam in een dockingstation geplaatst. De gegevens worden dan geüpload naar een beveiligde omgeving in de cloud. Via Evidence.com zijn de beelden (via account inlog) in te zien.

Inzien/overdragen

Zodra het beeldmateriaal is opgeslagen, mag dit door slechts een limitatief aantal personen in bepaalde functies geraadpleegd worden. In slechts drie gevallen mag het beeldmateriaal worden ingezien dan wel worden verstrekt, namelijk:

- Bij een klacht tegen het handelen van een handhaver, waarbij beelden van dit handelen zijn gemaakt;
- Bij een inzageverzoek door de gefilmde burger.

- Bij een vordering door de officier van justitie in het geval van een strafbaar feit, ten behoeve van de opsporing.
- Als de medewerker een geëscaleerde situatie wil evalueren.

Het beeldmateriaal wordt 28 dagen bewaard en daarna automatisch gewist, tenzij één van de eerste drie bovenstaande procedures/situaties van toepassing is. In deze 28 dagen moet zijn gebleken of er een klacht tegen een handhaver is ingediend, een inzageverzoek is ingediend door de betrokkene of er een vordering is gedaan door de officier van justitie. In dergelijke gevallen kan het beeldmateriaal langer bewaard worden, zolang als dit voor afhandeling van de zaak noodzakelijk is. Alle handelingen worden gelogd en kunnen bij twijfel en voor het uitvoeren van audits door bevoegde personen worden opgevraagd. Hierdoor blijft de privacy van de burgers en handhavers gewaarborgd.

Er wordt gebruik gemaakt van software, waarbij privacygevoelige informatie van derden (onder andere gezichten van anderen, kenteken en/of huisnummers) onzichtbaar dan wel onherkenbaar gemaakt kunnen worden (blurren).

4. Verwerkingsdoeleinden

Beschrijf de doeleinden van de voorgenomen gegevensverwerkingen.

Doel van de bodycam kan als volgt worden opgesomd:

- Versterken van de veiligheidsgevoelens van Handhavers VTH
- Het beperken en voorkomen van psychosociale arbeidsbelasting bij Handhavers VTH
- Bijdragen aan de-escalatie bij dreigende situaties gericht tegen Handhavers VTH
- De Handhavers VTH de mogelijkheid bieden om te leren van situaties die zijn vastgelegd. Alleen op verzoek van de betrokken Handhaver VTH uitsluitend met als doel van de situatie te leren zodat een volgende escalatie kan worden voorkomen of worden beperkt en zonder dat dit op enige wijze gevolgen heeft op de rechtspositie van de Handhaver VTH. Dit is een gerechtvaardigd belang waarmee we aansluiting vinden bij het bejegeningprotocol VTH. Van handhavers VTH wordt verwacht dat zij openstaan voor zelfreflectie.

Ondanks alle maatregelen (zowel landelijk als lokaal) om agressie en geweld een halt toe te roepen blijft er een verhoogd risico bij de uitvoering van toezichthoudende en handhavende taken. Jaarlijks wordt gerapporteerd op agressie en geweldsmeldingen in het Handhavingsverslag. Het melden van agressie en geweld is altijd een aandachtspunt van het management. Een recent medewerkers onderzoek gaf 77% van de medewerkers maandelijks of vaker in gevaarlijke situaties terecht te komen.

	2015	2016	2017	2018	2019	2020 (t/m 7 juni)
GIR-meldingen	62	78	27	56	49	45
Aanhoudingen	12	11	19	15	22	15
Geweldsmeldingen (geweld gebruikt door boa)	13	16	32	35	24	18

Agressie en geweld kunnen ernstige gevolgen hebben voor de medewerker, zowel mentaal als fysiek. De fysieke gevolgen kunnen variëren van lichte verwondingen, permanente fysieke gevolgen tot in potentie het overlijden. De gevolgen van verbale vormen van agressie is wellicht minder schadelijk, maar komen veel vaker voor. Dit kan leiden tot psychische pijn en andere gezondheidsklachten zoals:

- angstgevoelens;
- slaapstoornissen;
- maagpijn; en
- psychosomatische klachten.

Agressie en geweld zijn volgens de Arboret een vorm van psychosociale arbeidsbelasting.

Werkgevers zijn, zoals beschreven in artikel 2.15 Arbobesluit, verplicht maatregelen vast te stellen en uit te voeren om psychosociale arbeidsbelasting te voorkomen of indien dat niet mogelijk is te beperken.

Onderzoek

Uit verschillende onderzoeken wordt weergegeven dat de invoering van de bodycam heeft geleid tot een reductie van het aantal incidenten met 20% tot 50%. De evaluatie van Sander Flight 'Evaluatie bodycams Landelijke Eenheid, Proeftuin bodycams Dienst Infrastructuur (2018)' concludeert het volgende "Geweld tegen politieambtenaren is gedaald in de twee geografische afdelingen die met bodycams werkten. Het aantal incidenten van lichamelijke agressie en serieuze bedreigingen is gehalveerd. Tevens is het veiligheidsgevoel verbeterd bij degenen die vaak met de bodycam werkten: hoe vaker de bodycam werd gedragen, hoe groter dat effect." In de evaluatie van de pilot bodycams in Rotterdam (2019) van Van Rhee, Van Toorn en Flight noemt de volgende conclusies:

- De afspraken over privacybescherming van de BOA's en de burgers voldeden: er zijn geen klachten of vragen over gekomen;
- De bodycams hebben een de-escalierend effect op agressie en geweld door burgers. Er hebben zich geen incidenten voorgedaan door negatieve reacties op de bodycams;
- Handhavers voelen zich iets veiliger door de bodycams;
- Uit het onderzoek is gebleken dat er veel draagvlak onder de medewerkers is voor de bodycams en bijna iedereen vindt dat ze onderdeel moeten worden van de standaarduitrusting;
- De techniek heeft goed gewerkt: de bodycams en de beeldopslag voldeden goed;
- De spelregels over het wel of niet dragen en het maken van opnames moeten beter worden uitgelegd en meer worden nageleefd.

5. Betrokken partijen

Benoem welke organisaties betrokken zijn bij welke gegevensverwerkingen. Deel deze organisaties per gegevensverwerking in onder de rollen: verwerkingsverantwoordelijke, verwerker, verstrekker en ontvanger. Benoem tevens welke functionarissen binnen deze organisaties toegang krijgen tot welke persoonsgegevens.

- Gemeente Utrecht – gegevensverantwoordelijke
- Axon – verwerker
Axon technisch personeel zal alleen toegang hebben na uitdrukkelijke goedkeuring van Gemeente Utrecht. Dit zal alleen gebeuren als daar een technische reden aan ten grondslag ligt.
- Officier van Justitie – ontvanger
Alleen bij een vordering in het geval van een strafbaar feit, ten behoeve van de opsporing.

6. Belangen bij de gegevensverwerkingen

Beschrijf alle belangen die de verwerkingsverantwoordelijke en anderen hebben bij de voorgenomen gegevensverwerkingen.

Belang Gemeente Utrecht

Als werkgever hecht de gemeente Utrecht een grote waarde aan het veiligheidsgevoel van de Handhavers VTH. Werknemers moeten veilig en gezond kunnen werken. In de Arbeidsomstandighedenwet staan de kaders en verplichtingen van werkgevers om Arbobeleid te voeren. De bodycam wordt aan deze medewerkers van VTH ter beschikking gesteld op basis van artikel 3 lid 1 onder b Arbeidsomstandighedenwet. Ondanks alle maatregelen, zowel landelijk als lokaal (landelijk beleid veilige publieke taak, bejegeningprotocol, opleidingen) om agressie en geweld een halt toe te roepen blijft er een verhoogd risico bij de uitvoering van toezichthoudende en handhavende taken. De bodycam wordt ingezet als persoonlijk beschermingsmiddel.

Belang betrokkene

De betrokkene heeft in deze situatie een tegengesteld belang. Waar de handhaver VTH wilt dat de situatie de-escalereert, wil de betrokkene in de meeste gevallen waarbij de bodycam wordt aangezet

juist dat de situatie escaleert, maar wilt niet dat dit vastgelegd wordt op beeld.

7. Verwerkingslocaties

Benoem in welke landen de voorgenomen gegevensverwerkingen plaatsvinden.

Nederland

8. Technieken en methoden van de gegevensverwerkingen

Beschrijf op welke wijze en met gebruikmaking van welke (technische) middelen en methoden de persoonsgegevens worden verwerkt. Benoem of sprake is van (semi-) geautomatiseerde besluitvorming, profilering of big data-verwerkingen en, zo ja, beschrijf waaruit een en ander bestaat.

Er is geen sprake van geautomatiseerde besluitvorming, profilering of big data-verwerkingen.

Technieken en methoden van gegevensverwerkingen

1. Bodycam

De bodycams gebruiken een Hardware Security Module (HSM) om een sleutel te genereren dat uniek is voor elke bodycam. De HSM sleutelkluis genereert voor elke camera een unieke sleutel/certificaat. Axon Evidence (het systeem) levert een certificaat met openbare sleutel aan de bodycam via het Axon Dock. Nadat de bodycam het certificaat heeft, worden alle video's (opgenomen beelden) versleuteld met een openbare sleutel. Wanneer een opname wordt gestart, wordt een symmetrische AES 256-bits sleutel gegenereerd door de authenticatie-chip van de bodycam. De symmetrische sleutel wordt gecodeerd met het openbare certificaat. Het ID van het certificaat en de gecodeerde symmetrische sleutel worden opgeslagen in een apart bestand. Geen enkele opname gebruikt dezelfde symmetrische sleutel. Nadat de opname is beëindigd, wordt de symmetrische sleutel verwijderd uit het vluchtige geheugen van de bodycam.

Er worden geen niet-versleutelde symmetrische sleutels op de bodycam opgeslagen. Deze codering biedt bescherming tegen herstel van de mediabestanden in situaties waarin een camera verloren gaat of in gevaar komt.

2. Overdracht naar de server

Wanneer een bodycam in een Axon Dock wordt geplaatst, worden het ID-certificaat en de gecodeerde symmetrische sleutel via een beveiligd geverifieerd kanaal naar de server gestuurd. Gegevens die naar Axon Evidence worden verzonden, worden tijdens overdracht versleuteld met behulp van versleuteling die voldoet aan de standaarden FIPS 140-2 gevalideerd TLS 1.2 (356-bit AES, RSA 2048 bit sleutel) en PFS.

Gegevens worden in rust op de server opgeslagen met een AES-256 versleuteling.

3. De server, het beheer en de toegang

Axon Cloud Services worden geleverd als SaaS dienst. Klanttoegang is via een web interface die toegankelijk is via standaard webbrowsers. Dit datacenter staat per definitie binnen de EU. Evidence.com biedt verschillende risicoprofielen en verschillende beveiligingsbehoeften. Veel van de toegangscontrolefuncties kunnen worden in- of uitgeschakeld of kunnen worden gewijzigd om aan een specifiek risiconiveau te kunnen voldoen. De standaardinstellingen voor deze beveiligingsfuncties zijn gekozen om een hoog beveiligingsniveau te bieden, met behoud van flexibiliteit en gemak. De gemeente Utrecht beheert autorisaties en rolgebaseerde toestemmingen op basis van het eigen risicoprofiel en behoeften.

Deze functionaliteiten kunnen geëvalueerd en afgestemd worden op (eventuele) unieke behoeften van de gemeente Utrecht. Denk hierbij aan aanpasbare wachtwoordvereisten, multi-factor authenticatie-opties en het beperken van toegang tot gedefinieerde IP-bereiken.

4. Logging

Alle activiteiten van beheerders en gebruikers worden gelogd binnen Evidence.com. Dit kan gaan om een gebruiker die beelden bekijkt, metadata van beelden beheert, workflows uitvoert, bewerking en redactie van beelden, toewijzen van cases en categorieën en een systematische verwijdering van verwerkingen. Daarnaast worden ook activiteiten van individuele gebruikers gelogd zoals wijzigingen in het gebruikersaccount en bewijs gerelateerde gebruikersacties. Naast bewijs gerelateerde gebruikersacties zal het gebruikersauditspoor ook mislukte aanmeldpogingen laten

zien, wanneer een gebruiker van zijn account is uitgesloten door meerdere mislukte aanmeldpogingen of wanneer het wachtwoord van een gebruiker is gereset of zijn account is geblokkeerd. Tevens wordt gecentraliseerde logging van serveraudits en bewaking van beveiligingsgebeurtenissen door de leverancier ingezet om verdachte activiteiten te detecteren en forensisch onderzoek te steunen.

Logging van beelden blijft onbeperkt toegankelijk, zelfs na verwijdering van beelden. Server- en gebeurtenissenlogboeken worden minimaal een jaar bewaard.

Tijdens de pilot gaan we maandelijks (of nav incidenten/signalen) een audit uitvoeren door Functioneer Beheer VTH. Alleen zij hebben toegang tot de logging, welke in Evidence.com wordt opgeslagen.

Aanvullende informatie oer de beveiligingsoverwegingen die zijn ingebouwd in Axon Cloud Services en Axon apparaten is te vinden op www.axon.com/security.

9. Juridisch en beleidsmatig kader

Benoem de wet- en regelgeving, met uitzondering van de AVG en de Richtlijn, en het beleid met mogelijke gevolgen voor de voorgenomen gegevensverwerkingen.

- Artikel 3 lid 1 onder b, artikel 3 lid 2 Arbeidsomstandighedenwet: In deze artikelen wordt de wettelijke plicht omschreven die de werkgever heeft om een beleid te voeren dat is gericht op de veiligheid en gezondheid van haar medewerkers, gelet op de stand van de wetenschap en professionele dienstverlening.
- Artikel 8 lid 1 Arbeidsomstandighedenwet: In dit artikel staat de verplichting voor de werkgever om ervoor te zorgen dat de werknemers doeltreffend worden ingelicht over de te verrichten werkzaamheden en de daaraan verbonden risico's, alsmede over de maatregelen die erop gericht zijn deze risico's te voorkomen of te beperken.
- Artikel 2.15 Arbeidsomstandighedenbesluit: In dit artikel wordt beschreven dat de werkgever maatregelen moet treffen psychosociale arbeidsbelasting te voorkomen en als dit niet mogelijk is te beperken.
- Wet op de ondernemingsraden (art. 27): In dit artikel staat er instemming van de ondernemingsraad nodig is bij het voorgenomen besluit op het gebied van klachten afhandeling en de verwerking van persoonsgegevens.
- Artikel 7:611 BW dit artikel luidt: De werkgever en werknemer zijn verplicht zich als een goed werkgever en een goed werknemer te gedragen.
- Beleidsregels bodycams.
- Bejegeningprotocol VTH: hierin staat op welke wijze Handhavers VTH de-escalerend werken en hoe zij door middel van zelfreflectie hun handelen evalueren.

10. Bewaartermijnen

Bepaal en motiveer de bewaartermijnen van de persoonsgegevens aan de hand van de verwerkingsdoeleinden.

De pre-recorded beelden worden niet bewaard als de medewerker geen beelden heeft opgenomen (de bodycam niet heeft geactiveerd).

Het opgenomen beeldmateriaal wordt na activering van de bodycam 28 dagen bewaard en daarna automatisch gewist, tenzij:

- Er aangifte is gedaan van een incident waarbij de beelden als bewijsmateriaal kunnen dienen en het voor afhandeling van de zaak noodzakelijk is om deze beelden langer te bewaren.
- De betrokkene een klacht heeft ingediend.
- De betrokkene een inzageverzoek heeft ingediend.
- De beelden zijn gevorderd door de officier van justitie in het kader van het opsporingsonderzoek.

Beoordeling rechtmatigheid gegevensverwerkingen

Beoordeel de rechtsgrond, noodzaak en doelbinding van de voorgenomen gegevensverwerkingen en rechten van de betrokkene.

11. Rechtsgrond
<i>Bepaal op welke rechtsgronden de gegevensverwerkingen worden gebaseerd. Indien bijzondere of strafrechtelijke persoonsgegevens worden verwerkt, beoordeel of één van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing is. Bij verwerking van een wettelijk identificatienummer beoordeel of dit is toegestaan.</i>
Voor de privaatrechtelijke taak kan de gemeente zich tevens beroepen op de grondslag 'gerechtvaardigd belang' artikel 6, lid 1 onder f van de AVG. Dat is in deze veiligheid van de Handhavers VTH. Onder proportionaliteit en subsidiariteit wordt dit nader onderbouwd. De grondslag voor het verwerken ligt in de privaatrechtelijke taak van de gemeente. Vanuit een wettelijke plicht, namelijk een passende invulling van artikel 3 lid 1 onder b en 3 lid 2 van de Arbowet (wettelijke plicht van de werkgever om een beleid te voeren dat is gericht op de veiligheid en gezondheid van haar medewerkers) en artikel 2.15 van het Arbobesluit (werkgever moet maatregelen treffen om psychosociale arbeidsbelasting te voorkomen of beperken). (artikel 6, lid 1 onder c van de AVG) De bodycam past ook binnen het algemene kader van VTH (bejegeningprotocol), waarbij de-escalatie en zelfreflectie op het handelen een voorname leidraad vormt.
12. Doelbinding
<i>Indien 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.</i>
In voorkomend geval kunnen opgeslagen beelden worden gevorderd door de officier van justitie. De grondslag is het uitvoeren van een wettelijke plicht. De gemeente zal de gegevens voor geen ander doel gebruiken.
13. Juistheid
<i>Beoordeel de kwaliteit van de te verwerken gegevens.</i>
De bodycam is altijd stand-by maar wordt geactiveerd wanneer de Handhavers VTH in situaties terechtkomen die dreigen te escaleren of zijn geëscaleerd. Het filmen met een bodycam is feitelijk een observatie met behulp van een technisch middel: een vorm van versterkte waarneming. De camera registreert datgene waarop hij gericht is, in veel gevallen de gebeurtenissen die de medewerker van VTH zelf meemaakt, ziet en/of hoort. Hiermee kan met vrijwel 100% zekerheid geconcludeerd worden dat de juiste gegevens worden verwerkt.
14. Noodzaak en evenredigheid
<i>Beoordeel of de voorgenomen gegevensverwerkingen noodzakelijk zijn voor het verwezenlijken van de verwerkingsdoeleinden. Ga hierbij in ieder geval in op proportionaliteit en subsidiariteit.</i>
a. <i>Proportionaliteit: staat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden?</i> b. <i>Subsidiariteit: kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkenen minder nadelige wijze, worden verwezenlijkt? Benoem hierbij de overwogen alternatieven.</i>
<u>Proportionaliteit</u> Handhavers VTH hebben een publieke taak en moeten veilig kunnen werken. Meestal lukt dat ook, maar soms ontstaan er onveilige situaties waarin mensen agressief worden en zo een bedreiging vormen voor de Handhavers VTH. Als een situatie niet dreigt te escaleren of niet escaleert zal de

camera niet worden geactiveerd. Pas als er een voor de Handhaver VTH een onveilige situatie ontstaat wordt de bodycam geactiveerd. De burger wordt zoveel mogelijk vooraf gewaarschuwd voor activatie van de bodycam, hierdoor heeft de burger de kans zijn gedrag aan te passen en kan hij vastleggen door middel van de bodycam voorkomen. Gelet op de invloed die de burger zelf kan hebben op het activeren van de bodycam en gelet op het doel van de bodycam (de-escalatie en veiligheidsgevoel) kan worden gesteld dat de verwerking proportioneel is.

De beelden zijn voorzien van encryptie en worden opgeslagen op een beveiligde server waardoor ze niet zomaar uitgelezen kunnen worden. Voor het uitlezen is een protocol opgesteld, waarin onder meer wordt vermeld dat de beelden slechts na belendmaking aan het afdelingshoofd door een selecte groep, die is benoemd in het uitleesprotocol, kunnen worden bekeken. De beelden mogen niet verspreid worden via internet of social media. Door de strikte voorwaarden die gesteld worden aan het gebruik van de bodycams in combinatie met de doelstellingen waarvoor deze wordt ingezet wordt voldaan aan het proportionaliteitsbeginsel.

Afgelopen jaren zijn meerdere onderzoeken gedaan en hierin is te zien dat er een landelijke toename is in agressie, intimidatie en geweld jegens toezichthouders en BOA's. Een recent onderzoek bevestigt dit ook. In de openbare ruimte voelen Handhavers VTH zich onvoldoende beschermd ondanks de aanwezigheid van openbare orde camera's. Bovendien dekken de camera's niet de gehele stad, nemen deze geen geluid op en hebben vaak andere doelstellingen dan de bescherming van de Handhavers VTH. Voor de invoering van de bodycam is er onder de medewerkers een onderzoek uitgevoerd over het draagvlak. Daarbij gaf 88% van de medewerkers aan graag een bodycam te willen. 92% van de medewerkers gaf aan positief tegenover de bodycam te staan. Uit onderzoeken van andere gemeenten wordt weergegeven dat de invoering van de bodycam bij BOA's heeft geleid tot een reductie van het aantal incidenten met 20% tot 50%. Tevens is het veiligheidsgevoel verbeterd bij degenen die vaak met de bodycam werkten: hoe vaker de bodycam werd gedragen, hoe groter dat effect. Het is een proportioneel middel omdat mensen zich bewust zijn van het feit dat zij gefilmd worden en dan eerder geneigd zijn zich te gedragen. Dit werkt dus aan de voorkant de-escalerend.

Ook achten we de inzet ethisch verantwoord. Het gebruik van de bodycams belemmert betrokkenen niet in vrijheden die maatschappelijk geaccepteerd zijn.

Subsidiariteit

De veiligheid van de BOA heeft voortdurend bijzondere aandacht. Sinds 2009 heeft het management van VTH een vastgesteld bejegeningprotocol met de uitgangspunten hoe de handhavers van VTH horen te handelen. De-escalerend werken is daarbij het kernprincipe. De uitgangspunten zijn:

- Ik praat waar mogelijk
- Ik handel weloverwogen
- Ik pak door waar nodig
- Ik herken de situatie waarbij ik de politie moet inschakelen
- Ik sta open voor zelfreflectie

Het bejegeningprotocol biedt concrete handvatten, waarmee de Handhavers VTH de-escalerend kan optreden. Het protocol geldt als basis voor alle opleidingen en inwerkprogramma's van de Handhavers VTH.

Er wordt met regelmaat aandacht besteed aan de veiligheid van de Handhavers VTH en er worden maatregelen getroffen. Alle Handhavers VTH worden opgeleid om de-escalerend op te treden. Echter behelst de huidige uitrusting van de Handhavers VTH tot op heden geen vergelijkbaar middel dat kan worden ingezet om te voorkomen dat situaties escaleren. We zien dit als het minst zware middel om binnen de huidige wetgeving te kunnen inzetten om de psychosociale arbeidsbelasting bij Handhavers VTH te beperken.

15. Opslag

Beoordeel of de gegevens van alle verwerkingen niet langer dan noodzakelijk bewaard worden.

De opslag van data wordt alleen toegestaan op de bodycam en voor de opslag bestemde servers in de cloud. Het datacenter staat binnen de EU (Dublin).

Het beeldmateriaal wordt in beginsel 28 dagen bewaard en daarna automatisch gewist, tenzij één van de vier bovenstaande procedures/situaties van toepassing is. In dergelijke gevallen kan het beeldmateriaal langer bewaard worden, zolang als dit noodzakelijk is voor afhandeling van de zaak.

16. Bescherming

Beoordeel of alleen geautoriseerde medewerkers en externe partners/leveranciers toegang hebben tot de gegevens. Geef op hoofdlijnen en in lekentaal weer hoe de gegevens beschermd zijn tegen ongeautoriseerd gebruik.

- 1 De volgende medewerkers van de vigerende VTH organisatie mogen de beelden uitkijken:
 - a. Afdelingshoofd
 - b. Teamleider
 - c. Assistent teamleider
 - d. Senior hoofdinspecteur
 - e. Hoofdinspecteur
 - f. Medewerkers van de afdelingsondersteuning (klachtafhandelaar)
 - g. senior boa's
 - h. medior boa's
 - i. boa's
 - j. (senior) toezichthouders
 - k. Inspecteurs
2. Het uitkijken van de beelden geschied nooit individueel, maar altijd samen met een andere medewerker. Bij het uitkijken van de beelden zijn altijd minimaal aanwezig een medewerkers zoals bedoelt in lid 1 onder a, b, c, d, en f.
3. Medewerkers bedoelt onder lid 1 onder e, h, i, j en k mogen alleen beelden bekijken waar ze zelf opstaan of die zij zelf hebben opgenomen.
4. Het doel mag uitsluitend zijn:
 - a. Klachtafhandeling
 - b. Leerervaring op het plaatsgevonden incidentDe volgende maatregelen worden genomen bij het uitkijken van de beelden:
 1. Bij het uitkijken van de beelden wordt bewaakt dat geen andere derden dan de uitkijkende medewerkers beeldopname kan waarnemen.
 2. Bij het uitkijken van de beelden mag op geen enkele wijze beelden, foto's, geluidsopnames of kopieën worden gemaakt. Mocht dit gebeuren dan wordt het uitkijken direct beëindigd en melding gemaakt bij het Afdelingshoofd of diens plaatsvervanger. Op verzoek kunnen de beelden worden verstrekt zoals bedoeld in artikel 15 lid 3 AVG, met in acht neming van artikel 15 lid 4 AVG.
 3. Het afdelingshoofd, of diens plaatsvervanger, wordt vooraf voor het uitkijken is begonnen schriftelijk op de hoogte gesteld.

Uitlezen door anderen dan werkgever

1. Betrokken burger en/of diens belangenbehartigers mogen beelden bekijken:
 - a. Zij mogen de beelden alleen inzien als zij (vermoedelijk) zijn opgenomen met de bodycam.
 - b. De beelden mogen opgevraagd worden in kader van het recht op inzage zoals beschreven in artikel 15 lid 3 AVG.

- c. Bij het uitkijken van de beelden is altijd een medewerker van de vigerende handhavingsorganisatie zoals bedoeld onder lid 1 onder a, b,c, d of f aanwezig.
 - d. Op verzoek kunnen de beelden worden verstrekt zoals bedoeld in artikel 15 lid 3 AVG, met in acht neming van artikel 15 lid 4 AVG.
 - e. Het afdelingshoofd, diens plaatsvervanger, wordt vooraf voor het uitkijken is begonnen schriftelijk op de hoogte gesteld.
2. De officier van justitie kan in het kader van strafrechtelijk onderzoek beelden vorderen:
- a. Hiervoor dient een schriftelijke vordering te worden verstrekt
 - b. De beelden worden overgedragen conform de strekking van de vordering uit lid 1 onder a.
 - c. Het afdelingshoofd, of diens plaatsvervanger, wordt vooraf voordat het beeldmateriaal is overgedragen schriftelijk op de hoogte gesteld

Informatiebeveiliging

Opslag op de bodycam

- Het beeldmateriaal wordt versleuteld opgeslagen (encryptie, AES 128 XTS). Dit zorgt ervoor dat het beeldmateriaal beveiligd is tegen misbruik door onbevoegden.
- Het beeldmateriaal is opgeslagen op een niet-verwisselbare interne geheugenkaart. Dit zorgt ervoor dat de geheugenkaart van de bodycam bij diefstal of vernieling (nog afgezien van de encryptie) niet eenvoudig verwijderd en uitgelezen kan worden. De bodycams maken gebruik van een solid-state, niet-verwijderbare, geïntegreerde Multimedia Card (eMMC). eMMC-opslagmedia zijn direct op de printplaat aanwezig, waardoor het zeer moeilijk is om toegang te krijgen tot het opslagmechanisme zonder dat de camera wordt vernietigd.
- Om verdere toegang te vermoeilijken is het belang dat de camera's geen gebruik maken van standaard-multimedia aansluitingen. Het beeldmateriaal is niet zonder speciale kabel van de leverancier op een computer aan te sluiten. Deze speciale kabel is niet verkrijgbaar bij een elektronicawinkel.

Aan het einde van de dienst wordt de bodycam door de Handhaver VTH in het dockingstation gezet. Het opgeslagen beeldmateriaal wordt op dat moment versleuteld naar de server verzonden en opgeslagen.

Ook hier zijn diverse maatregelen genomen om misbruik te voorkomen:

- Het beeldmateriaal wordt versleuteld (encryptie) verzonden naar de server, waardoor dit beveiligd is tegen misbruik door onbevoegden.
- Zodra het beeldmateriaal is opgeslagen, mag dit door slechts een limitatief aantal personen in bepaalde functies geraadpleegd worden.
- In slechts drie gevallen mag het beeldmateriaal worden ingezien dan wel overgedragen, namelijk:
 - Bij een klacht tegen het handelen van een handhaver, waarbij beelden van dit handelen zijn gemaakt;
 - Bij een inzageverzoek door de gefilmde burger.
 - Bij een vordering door de officier van justitie in het geval van een strafbaar feit, ten behoeve van de opsporing. Beeldmateriaal wordt dan beveiligd middels zivver verstuurd.
 - Als de medewerker een geëscaleerde situatie wil evalueren.
- Alle handelingen worden gelogd en kunnen bij twijfel of bij audits door hiertoe bevoegde personen worden opgevraagd. Hierdoor blijft de privacy van de burgers en handhavers gewaarborgd.
- Er wordt gebruik gemaakt van software, waarbij privacygevoelige informatie van derden (onder andere gezichten, kenteken en/of huisnummers) onzichtbaar dan wel onherkenbaar maakt (blurren). Ook dit zorgt ervoor dat de privacy van burger gewaarborgd blijft.

Toegang tot Evidence.com wordt belegd bij functioneer beheer van VTH en wordt uitgevoerd conform het toegangsbeheer proces van VTH. Wachtwoordinstellingen worden ingericht conform het beleid accounts en authenticatiemiddelen v1.0. De leverancier is in staat om per vertrouwelijkheidsniveau te voldoen aan de eisen van gemeente ten aanzien van authenticatiemiddelen.

17. Rechten van de betrokkenen

Geef aan hoe invulling wordt gegeven aan de rechten van de betrokkenen. Indien de rechten van de betrokkene worden beperkt, bepaal op grond van welke wettelijke uitzondering dat is toegestaan.

Op www.utrecht.nl/privacy kan een ieder inzien hoe de gemeente Utrecht omgaat met gegevens en welke rechten een betrokkene heeft.

- Recht op informatie: De toezichthouder of boa waarschuwt voordat hij de bodycam aanzet en legt uit waarom hij dit doet, mits de situatie dit toe laat. Daarnaast zal informatie over de bodycam worden opgenomen op de website. De verwerking nemen we tevens op in het verwerkingsregister.
- Recht op inzage: De betrokkene heeft de mogelijkheid tot inzage in zijn gegevens. Hiervoor is een gemeentelijk inzageproces voor opgesteld.
- Recht op rectificatie: Aanvragen voor correctie worden in behandeling worden genomen door de verwerkingsverantwoordelijke.
- Recht op gegevenswissing: Betrokkene heeft recht om dit verzoek te doen.
- Recht op beperking van de verwerking: Er is in beginsel al rekening gehouden met dataminimalisatie. Het beperken van verwerking is niet mogelijk omdat de genoemde gegevens minimaal nodig zijn.
- Recht van bezwaar: De betrokkene heeft het recht om in bezwaar te gaan.

C. Beschrijving en beoordeling risico's voor de betrokkenen

Beschrijf en beoordeel de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Houd hierbij rekening met de aard, omvang, context en doelen van de voorgenomen gegevensverwerkingen.

18. Risico's
<i>Beschrijf en beoordeel de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Ga in ieder geval in op:</i> <i>a. welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen;</i> <i>b. de oorsprong van deze gevolgen;</i> <i>c. de waarschijnlijkheid (kans) dat deze gevolgen zullen intreden;</i> <i>d. de ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden.</i>
1) Gedrag van de betrokkene wordt vastgelegd en hierdoor bestaat het risico dat de beelden verkeerd worden geïnterpreteerd (valse beschuldiging/stigmatisering). 2) De betrokkene loopt een groter risico om gefilmd te worden in de openbare ruimte aangezien er ook al openbare orde camera's zijn. 3) De betrokkene wordt onrechtmatig gefilmd door de BOA. 4) Beelden komen op straat te liggen doordat de leverancier wordt gehackt. 5) Er hebben andere mensen toegang tot de gegevens (zoals de leverancier) dan wij hebben vastgesteld. 6) Beelden worden langer bewaard dan afgesproken. 7) Artikel 32 AVG vraagt om verantwoording en aantoning van passende technische en organisatorische maatregelen om het beveiligingsniveau te waarborgen. Het is onduidelijk of de leverancier op dit moment over alle noodzakelijke documentatie beschikt waarmee aangetoond kan worden dat voldaan wordt aan deze verplichting.

D. Beschrijving voorgenomen maatregelen

Beschrijf de voorgenomen maatregelen om de hiervoor beschreven risico's van de voorgenomen gegevensverwerkingen voor de vrijheden en rechten van de betrokkenen aan te pakken.

19. Maatregelen

Beoordeel of de reeds getroffen maatregelen, beschreven onder '16. Bescherming', afdoende zijn. Beoordeel welke technische, organisatorische en juridische maatregelen in redelijkheid kunnen worden getroffen om de hiervoor beschreven risico's te voorkomen of te verminderen. Beschrijf welke maatregel welk risico aanpakt en wat het restrisico is na het uitvoeren van de maatregel. Indien de maatregel het risico niet volledig afdekt, motiveer waarom het restrisico acceptabel is.

- 1) De handhaver zet de bodycam pas aan als er sprake is van escalatie waardoor zijn veiligheidsgevoelens in het geding komen. Om de situatie niet verkeerd te interpreteren of de betrokkene vals te beschuldigen wordt door middel van pre-recording (tot max 120 seconden) ook de aanleiding van de situatie gefilmd. Daarbij maakt een medewerker, bij het maken van beelden met de bodycam, altijd een proces verbaal waarin hij de feiten en omstandigheden beschrijft die hebben geleid tot het gebruik en de situatie is die vastgelegd. Bij een BOA gebeurt dit ook nog een op ambtseed, waardoor het stand houdt in de rechtbank.
- 2) In de openbare ruimte voelen toezichthouders en boa's zich onvoldoende beschermd ondanks de aanwezigheid van openbare orde camera's. Bovendien dekken de camera's niet de hele stad en hebben vaak andere doelstellingen dan de bescherming van handhavers van VTH.
- 3) Voor het gebruik van de bodycam hebben we een duidelijk protocol opgesteld met richtlijnen. Telkens als ervoor gekozen wordt om de bodycam aan te zetten en de beelden worden opgeslagen, dient de medewerker van VTH dit gebruik vast te leggen in een proces verbaal waarbij verslag wordt gemaakt van de situatie en de redenen die ertoe hebben geleid. Dit om het gebruik van de bodycam te verantwoorden.
- 4) De leverancier heeft enkel toegang tot de beelden indien hier nadrukkelijk goedkeuring voor is gegeven vanuit de gemeente en hier een technische reden ten grondslag ligt. Zie daarnaast de maatregelen die omschreven zijn in onderdeel 15 en 16. Middels logging wordt dit gecontroleerd.
- 5) De leverancier heeft enkel toegang tot de beelden indien hier nadrukkelijk goedkeuring voor is gegeven vanuit de gemeente en hier een technische reden ten grondslag ligt. Zie daarnaast de maatregelen die omschreven zijn in onderdeel 15 en 16. Middels logging wordt dit gecontroleerd.
- 6) In de techniek is een bewaartermijn geregeld. De beelden worden na dit bewaartermijn automatisch verwijderd. Bij enkel drie uitzonderingen (zie onderdeel 10) zullen beelden langer worden bewaard.
- 7) De leverancier wordt gevraagd inzage te geven in de documentatie, dan wel deze op te stellen om aan te tonen dat aan artikel 32 AVG wordt voldaan. Daarbij wordt een verwerkersovereenkomst afgesloten met de leverancier en is de leverancier in het bezit van een intern privacyreglement. De leverancier is tevens in het bezit van de volgende certificeringen:
 - ISO/IEC 27001:2013 Certified
 - ISO/IEC 27018:2014 Certified
 - CJIS Compliant
 - CALEA Standard 17.5.4 Compliance
 - HIPAA and HITECH
 - SOC 2+ Report
 - Cloud Security Alliance – CSA STAR Attestation (Level Two)

- Cloud Security Alliance – CSA STAR Self-Assessment (Level One)
- Accessibility Conformance Report – WCAG 2.0 & VPAT/Section 508
- Federal Risk and Authorization Management Program (FedRAMP)

Conclusie

De restrisico's ten aanzien van de rechten en vrijheden van de betrokkene zijn acceptabel.