

Rapportage Data Protection Impact Assesment Cameratoezicht Veen

Inhoud

Managementsamenvatting	3
Aanleiding.....	3
Inhoud	3
Oordeel Functionaris gegevensbescherming	4
Omschrijving van de verwerking en de context.....	6
Doelen en verantwoordelijkheden van de verwerking	6
Gegevens, processen en de levenscyclus ondersteunende systemen	8
Beschrijving van de systemen, technieken en methoden voor gegevensverwerking.....	8
Toetsing evenredigheid en noodzaak	8
Toetsing rechten van betrokkenen.....	9
Toetsing verwerkers en gegevensoverdracht	10
Bijlage Overzicht risico's voor betrokkenen.....	10

Managementsamenvatting

Aanleiding

De verwerkingsverantwoordelijke moet voorafgaand aan een verwerking van persoonsgegevens waar mogelijk hoge risico's voor betrokkenen aan verbonden zijn een data protection impact assessment (DPIA) uitvoeren om de waarschijnlijkheid en ernst van deze risico's te beoordelen. Hierbij moet rekening worden gehouden met de aard, omvang, context en doelen van de gegevensverwerking en de bronnen van de risico's. Bij een DPIA moet met name worden gekeken naar de geplande maatregelen, waarborgen en mechanismen om risico's te beperken, de persoonsgegevens te beschermen en aan te tonen dat aan de Algemene Verordening Gegevensbescherming (AVG) wordt voldaan.

Een DPIA is een proces dat is bedoeld om de gegevensverwerking van persoonsgegevens te beschrijven, de noodzaak en evenredigheid ervan te beoordelen en de daaraan verbonden risico's voor de rechten en vrijheden van natuurlijke personen te helpen beheren. Hiervoor moeten risico's worden ingeschat en maatregelen worden bepaald om deze risico's aan te pakken. Een DPIA is dus een belangrijk verantwoordingsinstrument. Het helpt verwerkingsverantwoordelijken om aan de eisen van de AVG te voldoen, en om aan te tonen dat passende maatregelen zijn genomen om ervoor te zorgen dat de AVG wordt nageleefd. Met andere woorden: een DPIA is een proces voor het realiseren en aantonen van naleving.

Inhoud

Deze rapportage gaat over Cameratoezicht Veen proces en bevat de uitkomsten van het Data Protection Impact Assessment(DPIA) van Cameratoezicht Veen in de vorm van een rechtmatigheidstoets en een beoordeling van de belangrijkste bedreigingen die van invloed zijn op het proces en de schatting van de risico's voor betrokkenen die verbonden zijn aan deze verwerking. Op basis van deze risico-inschatting zijn vervolgens tegenmaatregelen bepaald die van toepassing zijn op het proces en geïmplementeerd moeten worden. Deze Analyse is afgerond op 28-11-2022

Oordeel Functionaris gegevensbescherming

Ruimte voor beoordeling van de verwerking door de FG

Er is een aangetoonde noodzaak voor cameratoezicht. Aan de eisen van artikel 151c gemeentewet is ook aantoonbaar voldaan en er zijn beperkende maatregelen genomen. Uit maatregelen in het verleden is gebleken dat alternatieven niet goed werkten. De verwerking is tot het minimum beperkt. Voor de motivering kan naar de DPIA worden verwezen. Er bestaan geen bezwaren tegen deze verwerking. Wel moet er nog gekeken worden naar de verwerkersovereenkomst met Solid Systems. Ook mogen de uitzonderingen van artikel 41 UAVG niet ruimer gebruikt worden dan absoluut noodzakelijk. Maw,... wanneer er persoonsgegevens worden verwerkt na de bewaartermijn en er geen gevaar meer is voor de openbare orde dan moeten inwoners van het bestaan van de beelden op de hoogte worden gebracht. Tot slot is het advies om te werken met een eenvoudige autorisatiematrix waarin is aangegeven wie van de verkenningseenheid precies toegang heeft op welk moment. Voor het overige is het advies positief.

Middels ondertekening van dit document worden deze risico's geaccepteerd door de verantwoordelijke en goedgekeurd door de functionaris gegevensbescherming.

De analyse is opgesteld door [REDACTED] in overleg met de volgende personen:

Naam..... Functie....

.....

.....

De analyse is aangeboden aan de functionaris gegevensbescherming:

Naam.....

Handtekening goedkeuring

.....

De analyse is aangeboden aan de verantwoordelijke:

Naam..... Functie....

.....

Handtekening risico-acceptatie

.....

Omschrijving van de verwerking en de context

De AVG vereist dat een systematische beschrijving van de gegevensverwerking wordt gegeven en dat rekening wordt gehouden met de aard, omvang, context en doelen van de gegevensverwerking. Bij voorkeur wordt dit ingevuld door de proces- of systeemeigenaar. De beschrijving bevat ten minste een systematische beschrijving van de beoogde gegevensverwerkingen en de verwerkingsdoeleinden, waaronder de gerechtvaardigde belangen die door de verwerkingsverantwoordelijke worden behartigd. Hieronder is dat uitgewerkt.

Doelen en verantwoordelijkheden van de verwerking

Welke gegevensverwerking wordt overwogen?

Het betreft beeldmateriaal. Het gebied in en rond het kruispunt in Veen (Witboomstraat / Vd Loostraat / Mussentind) heeft al meerdere jaren te kampen met ernstige verstoringen van de openbare orde en veiligheid en de daarmee gepaard gaande overlast voor de omgeving die voornamelijk door bewoners en bezoekers van en rondom het 'kruispunt' veroorzaakt wordt. De jaarwisseling van 2021 op 2022 leidde tot een schadepost van meer dan 130.000 euro en tal van strafbare feiten. Om de openbare orde te bewaken en hulpverleners de mogelijkheid te geven hun taak uit te oefenen is cameratoezicht binnen het in het aanwijsbesluit genoemde gebied noodzakelijk. Het betreft het gebied dat wordt omsloten door de volgende straten: Grotestraat, Hofstraat, Van der Loosstraat, Mussentind, Witboomstraat, Singel, Hardenbergh, Wilhelminastraat, Mauritsstraat, Willem de Zwijgerstraat, Frederik Hendrikstraat, alles zoals weergegeven op de bij het aanwijsbesluit gevoegde kaart. Dit cameratoezicht is voor de periode van 1 december 2022 tot 4 januari 2023. Deze gegevens zullen tenminste 7 dagen worden opgeslagen. Dit tenzij er een ernstig vermoeden is van een strafbaar feit en de gegevens gevorderd worden door de politie dan wel het waarschijnlijk is dat de gegevens zullen worden gevorderd worden. In dit laatste geval is verlenging mogelijk met nogmaals zeven dagen. Deze beelden zullen worden gemaakt door Solid Systems en vervolgens worden gebruikt door een verkenningseenheid. Deze eenheid bestaat uit politie, brandweer en OvJ.

Wat zijn de doeleinden van de gegevensverwerkingen?

1. Bescherming openbare orde conform artikel 151c Gemeentewet.
2. Veilig uitoefenen publieke taak
3. Beperken schade aan particuliere en gemeentelijke eigendommen

Waar vinden de gegevensverwerkingen plaats?

De opslag zal primair plaatsvinden op een netwerkrecorder die op een geheime fysieke locatie is geplaatst. De opslag is daarmee lokaal en wordt niet in een cloud o.id gedeeld. Toegang tot live of opgenomen beeld, uitsluitend via de app (MV3000) die Solid Systems beschikbaar zal stellen. Hiervoor zal centraal een unieke toegangscode per dag worden gebruikt voor toegang door leden van de genoemde verkenningseenheid. Deze code wordt dan door de coördinatie van de betrokken diensten gedeeld naar de collega's die op die dag dienst hebben. Back-ups worden er in deze configuratie gemaakt en extern opgeslagen voor maximaal 7 dagen (met verlenging voor maximaal nogmaals zeven dagen). Solid systems is administrator op de recorder en verstrekt de wachtwoorden. Dit wordt gedaan door onze support afdeling waar iedere medewerker een VOG heeft en de informatie allemaal beveiligd is op hun gesloten netwerk. Alle verbindingen naar de recorder en camera gaan via een toegang uitsluitend met paswoord. Na de gebruiksperiode zal Solid Systems alle beelden wissen.

Welke verantwoordelijkheden zijn verbonden aan de gegevensverwerking?

De primaire grondslag is artikel 151c Gemeentewet. Aan de in dit artikel genoemde eisen moet worden voldaan.

Welke wet- en regelgevingen hebben betrekking op de gegevensverwerkingen?

Toepasselijke regelgeving - Algemene verordening gegevensbescherming (AVG) - Uitvoeringswet AVG (UAVG) - Wet politiegegevens (Wpg) - Gemeentewet (art. 151c) - EU: European Data Guidelines 3/2019 on processing of personal data through video devices, 10 juli 2019. - Beleidsregels cameratoezicht onder Wpg en Wbp / 9 februari 2016 AP.

Zijn er normen van toepassing op de gegevensverwerking?

BIO, WPG conform NOREA Audit gebruik WPG gegevens.

Gegevens, processen en de levenscyclus ondersteunende systemen

Welke persoonsgegevens worden verwerkt?

- * Beeldmateriaal (videomateriaal, audiomateriaal)
- * Locatiegegevens (lengtegraad, breedtegraad)

Welke bijzondere persoonsgegevens worden verwerkt?

Geen

Worden persoonsgegevens van kwetsbare groepen verwerkt?

Nee

Beschrijving van de systemen, technieken en methoden voor gegevensverwerking.

Hoe werkt de levenscyclus van persoonsgegevens en processen?

De beelden worden gemaakt vanaf een geheime locatie binnen het in het aanwijsbesluit genoemde gebied. Het is niet mogelijk de precieze locatie te noemen omdat er gegronde vrees bestaat dat bekendmaking hiervan tot sabotage zal leiden. Ook de netwerkrecorder is op een niet nader te noemen locatie geplaatst. De opslag hiervan is lokaal. De beelden zullen worden uitgelezen door leden van de verkenningseenheid. Op basis van de beelden kunnen de leden inschatten of er sprake is van een (dreigende) verstoring van de openbare orde en of dienstverleners veilig hun publieke taak kunnen uitoefenen. Indien nodig kan de politie de beelden vorderen. Normaliter zullen de beelden na zeven dagen gewist worden. De opslag van de back up zal bij Solid Systems plaatsvinden. Ook deze gegevens worden na de genoemde periode gewist.

Wat zijn de persoonsgegevens ondersteunende systemen?

De netwerkrecorder en het camerasysteem zijn van Solid Systems. De app betreft een externe leverancier. Nadere verwerking door leden van de verkenningseenheid is onbekend en valt buiten de scope van deze DPIA.

Welke technieken en methoden worden gebruikt voor de gegevensverwerking?

Camerabeeldtechnologie en opslagmedia door Solid Systems.

Toetsing evenredigheid en noodzaak

Zijn de verwerkingsdoeleinden gespecificeerd, expliciet en legitiem?

Ja. De grondslag is verstoring openbare orde. Veen kent een lange traditie van overlast tijdens de jaarwisseling. Zie bijvoorbeeld; <http://lokalezaken.com/wp/wp-content/uploads/2019/12/Veen-Wie-stookt-er-nou-maart-2005.pdf> . Er is een voorzienbare verstoring ook dit jaar en er is (gegronde) angst

bij brandweer en politie dat zij niet op een veilige manier hun taak kunnen uitoefenen. Voor een nadere toelichting van de belangen zie ook het aanwijbsbesluit.

Wat is de grondslag van de gegevensverwerking?

De grondslag is artikel 151c Gemeentewet in combinatie met artikel 2.77 APV. Aan de procedurele eisen zoals onder andere het overleg in artikel 151c gemeentewet lid 2 met de OvJ is voldaan. De bewaartermijn is korter aangehouden dan de genoemde 4 weken omdat er geen noodzaak lijkt te zijn voor langere bewaring. Er lijkt voldoende feitelijke aanleiding aanwezig te zijn om een (dreigende) verstoring van de openbare orde aan te nemen.

Zijn de persoonsgegevens adequaat, relevant en beperkt tot wat nodig is met betrekking tot de doeleinden waarvoor ze worden verwerkt ('gegevensminimalisatie')?

Er worden alleen opnames gemaakt van het risicogebied. Doel is bescherming openbare orde en veilige werkomgeving hulpverleners. Er worden slecht beperkt beelden gemaakt, binnen het minimaal noodzakelijke gebied, voor niet langer dan noodzakelijk en welke slechts toegankelijk voor een beperkte groep.

Zijn de persoonsgegevens juist en worden ze up-to-date gehouden?

Het betreft videobeelden. Daarbij is er de mogelijkheid om in te zoomen op persoonsniveau maar dat is niet het doel. Het doel is het beoordelen of er sprake is van een verstoring van de openbare orde. Verificatie zal plaatsvinden doordat na de initiële beoordeling ook indien nodig fysiek op de locatie aanwezig zal zijn.

Wat is de bewaartermijn van de persoonsgegevens?

De bewaartermijn van de beelden en de back-ups is zeven dagen. Dit tenzij het waarschijnlijk is dat de politie de beelden zal vorderen. In dat geval is verlenging mogelijk met nogmaals zeven dagen. Hierna zullen de gegevens gewist worden.

Toetsing rechten van betrokkenen

In dit deel wordt beschreven dat de nodige middelen worden ingezet om de betrokken personen in staat te stellen hun rechten uit te oefenen.

Is het voor betrokkenen helder wat er met zijn persoonsgegevens gebeurt en waarom?

Aan betrokkenen zal duidelijk gemaakt moeten worden dat er cameraopnames gemaakt worden. Dat hoeft niet te verwijzen naar een hele specifieke locatie maar wel een afgebakend gebied. Er zal aangegeven moeten worden dat er een besluit is genomen. Een ieder die het gebied binnenkomt, zal door middel van een bordje ervan op de hoogte worden gebracht dat er opnames gemaakt (kunnen) worden. Door bekendmakingen zal aan artikel 151c lid 4 Gemeentewet worden voldaan.

Hoe kunnen betrokkenen hun recht op toegang en overdraagbaarheid van persoonsgegevens uitoefenen?

Op grond van artikel 41 Uitvoeringswet AVG kan de verwerkingsverantwoordelijke de verplichtingen en rechten, bedoeld in de artikelen 12 tot en met 21 en artikel 34 van de verordening, buiten toepassing laten voor zover zulks noodzakelijk en evenredig is ter waarborging van: c.de openbare veiligheid; en d.de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid. Er is gebruik gemaakt van dit artikel. Indien beelden met herkenbare

persoonsgegevens opgeslagen of anderszins gebruikt worden en er geen gevaar meer is voor de openbare orde dan zullen individuen actief op de hoogte gebracht worden van het bestaan van de beelden.

Hoe kunnen betrokkenen hun recht op rectificatie en verwijdering uitoefenen?

Zie hierboven

Hoe kunnen betrokkenen hun recht op beperking uitoefenen en bezwaar maken?

Zie hierboven

Toetsing verwerkers en gegevensoverdracht

Beschrijving van de verantwoordelijkheden van een eventuele verwerker.

Zijn de verplichtingen van de verwerkers duidelijk geïdentificeerd en geregeld in een (verwerkers)overeenkomst?

Solid System verwerkt persoonsgegevens ten behoeve van de gemeente Altena. Er is sprake van een verwerkingsovereenkomst met Solid Systems. Dit is echter voor de bescherming van het gemeentehuis. Er zal bekeken moeten worden of de huidige verwerkingsovereenkomst voldoet voor dit specifieke doel van 151c gemeentewet.

Zijn de persoonsgegevens in het geval van gegevensoverdracht buiten de Europese Unie voldoende beschermd?

Solid Systems is gevestigd in Werkendam en heeft geen vestigingen buiten de AU. Voor het uitlezen van de beelden zal gebruik worden gemaakt van de app MV3000 van de ontwikkelaar Kuk Hyeong Kim. Dit bedrijf lijkt actief te zijn in Zuid Korea. Voor Korea is een adequacy decision van kracht; https://ec.europa.eu/info/files/decision-adequate-protection-personal-data-republic-korea-annexes_en . Dit wil zeggen dat het beschermingsniveau voor Zuid Korea op een gelijk niveau ligt als dit van de EU. Op deze grond is er sprake van voldoende bescherming.

Overzicht potentiële risico's voor betrokkenen

Dreiging	Categorie dreiging	Omschrijving dreiging	Netto kans	Netto schade
46	AVG rol onduidelijk	Je ziet jezelf als verwerker ipv verantwoordelijke of andersom (relatie Solid Systems, APP, verkenningseenheid, VTH)	3.85	7
15	Afluisteren	Afluisteren of spionage op afstand	3	7
24	Apparatuurstoring	Apparatuur functioneert niet meer volgens de specificaties	3.85	7

54	Betrokkene niet goed geïnformeerd over verwerking	Betrokkene is niet goed geïnformeerd over de verwerking van zijn persoonsgegevens. Let op uitzondering 41 UAVG.	3.95	7
17	Diefstal van apparatuur	Diefstal van apparatuur(laptops, telefoons e.d) die niet-openbare gegevens bevat	2.85	7
16	Diefstal van media of documenten	Diefstal van media of documenten die niet-openbare gegevens bevatten	2.85	7
53	Doel kan ook op een minder ingrijpende manier worden bereikt	Het doel kan ook op een (voor betrokkene) minder ingrijpende manier worden bereikt	3.85	7
68	Exporteren datasets is te gemakkelijk	Er kunnen te gemakkelijk rapportages met persoonsgegevens worden gemaakt	3.72	7
47	Function creep	Functie-uitbreiding waarbij PG voor ander doel verwerkt worden	3.85	7
22	Geavanceerde aanhoudende dreiging	Langdurige en doelgerichte cyberaanval waarbij een onbevoegd persoon onopgemerkt en langdurig toegang krijgt tot een netwerk. Het doel is om continu toegang te krijgen en gegevens te stelen. (netwerkrecorder op locatie maar mogelijk wel van toepassing voor back ups),	2.95	7
49	Gebrek aan sturing en verantwoordelijkheden	Onduidelijkheid wie in verkenningseenheid stuurt op informatiebeveiliging en de compliancy is niet belegd. Mogelijke verdere verwerkingen door deelnemers.	3.85	7
20	Geknoei met hardware	Aanpassingen doen aan hardware die de veiligheid beïnvloeden	5	7
78	Heimelijke verwerking persoonsgegevens	Persoonsgegevens worden heimelijk verwerkt, (kenbaarheid laat te wensen over)	4	7
31	Illegale verwerking van gegevens	(Persoons)gegevens verwerken die niet verwerkt mogen worden	3.85	7
33	Misbruik van rechten	Bewust misbruik maken van toegekende rechten	4	7
50	Doorzending derde landen	App komt uit Zuid Korea. Deze kent echter hoog beschermingsniveau.	3.85	7
63	Autorisaties	Onduidelijk is wie op welk moment toegang heeft	3.85	7
18	Onderschepping van gerecyclede of weggegooid media	Onderschepping van gerecyclede of weggegooid media die niet-openbare gegevens bevat	2.85	7
70	Onduidelijkheid over grondslag gegevensdeling	Door vermenging van taken is niet duidelijk welke grondslag van toepassing is (denk aan sociaal domein waar hulpverlenings- en gemeentelijke taken door elkaar lopen of aan de WPG)	3.72	7
28	Ongeoorloofd gebruik van apparatuur	Apparatuur gebruiken op een niet toegestane of onveilige manier	2.85	7
76				

74	Onnodig volgen betrokkenen	Personen worden onnodig gevolgd	3.85	7
34	Samenvoeging van rechten	Onterechte stapeling van rechten bij een gebruiker. Door slordigheid of bewuste toekenning.	4	7
27	Schending van onderhoudbaarheid van informatiesystemen	Geen ondersteuning/updates meer beschikbaar voor informatiesystemen	4	7
26	Vwo	Vwo voldoet niet of deels	3.88	7
67	Ta lang bewaren gegevens	Persoonsgegevens worden langer dan noodzakelijk bewaard, of langer dan de geldende bewaartermijn (gelijk aan 3)	3.85	7
71	Teveel toegang tot gegevens	Er wordt teveel, ten onrechte of te lang toegang gegeven tot informatie (waardoor bv teveel mensen toegang hebben)	3.72	7
62	Teveel vertrouwen in systeem	Medewerker gaat teveel vertrouwen op het systeem, waardoor hij zich als zodanig gaat gedragen, zoals het systeem hem adviseert.	3.72	7
79	Verwerking buiten zicht gebruiker	Er worden persoonsgegevens buiten het zicht gebruiker van de applicatie/app verwerkt (b.v. in metadata of diagnostic)	4	7
56	Verwerking in derde landen zonder afdoende aanvullende afspraken	Er worden gegevens uitgewisseld met landen waar persoonsgegevens onvoldoende zijn beschermd en er zijn onvoldoende aanvullende afspraken gemaakt	3.72	7
51	Verwerking zonder grondslag	Er worden persoonsgegevens verwerkt waarvoor geen grondslag aanwezig is	3.72	7

Alle risico's bevinden zich binnen te accepteren bandbreedte. Wel moet er extra aandacht zijn voor de fysieke bescherming van de netwerkrecorder.

Toelichting grondslagen

In dit document kunt u secties vinden die onleesbaar zijn gemaakt. Deze informatie is achterwege gelaten op basis van de Wet open overheid (Woo). De letter die hierbij is vermeld correspondeert met de bijbehorende grondslag in onderstaand overzicht.

J Art. 5.1 lid 2 sub e

Het belang van de openbaarmaking van deze informatie weegt niet op tegen het belang van de eerbiediging van de persoonlijke levenssfeer van betrokkenen