

BEPERKT TOEZICHTSONDERZOEK

**BEPERKT TOEZICHTRAPPORT DOOR HET
CONTROLEORGaan OP DE POLITIONELE
INFORMATIE IN HET RAAM VAN ZIJN CONTROLE- EN
TOEZICHTSBEVOEGDHEDEN N.A.V. HET DELEN VAN
CAMERABEELDEN VIA HET REAL TIME
INTELLIGENCE CENTER/OSINT-BESTUURLIJK
TUSSEN HET CIC OOST VLAANDEREN EN DE PZ
NINOVE**

Rapport

Referte: CON22003

**CONTROLEORGaan OP DE
POLITIONELE INFORMATIE**



0 Inhoudsopgave

1	INLEIDING	3
1.1	Management Summary	3
1.2	Kennisname van de feiten	4
2	TER HERINNERING – DE VISIE VAN HET COC	5
3	OPZET VAN HET TOEZICHT EN METHODOLOGIE	6
4	ONDERZOEKSBEVINDINGEN	8
4.1	Inleiding	8
4.2	Verhouding tussen de betrokken actoren	8
4.2.1	PZ Ninove en CSD OVL	8
4.2.2	DGR/DRI en Microsoft als verwerkers	9
4.2.3	Tein, Genetec en Edesix als verwerkers	9
4.3	Scope van het project	10
4.4	Rol van <i>MS Teams</i>	11
4.4.1	Algemeen	11
4.4.2	Traceerbaarheid en logging <i>MS Teams</i>	11
4.4.3	Controle op verdere verspreiding	11
4.4.4	Beleid rond mobiele toestellen waarop <i>MS Teams</i> geïnstalleerd is	12
4.4.5	Alternatieven voor <i>MS Teams</i>	12
4.5	Rol van CAD in de werkprocessen.....	14
4.6	Rol van ISLP in de werkprocessen	14
4.7	Profiel- en toegangsbeheer	14
4.8	Bewaartermijnen in de verschillende systemen	15
4.9	Logbestanden voor de verwerkingen in zijn geheel	15
4.10	Privacy-protocol.....	16
4.11	Didactisch gebruik van de camerabeelden	16
5	JURIDISCH – TECHNISCH – FUNCTIONEEL KADER	16
5.1	Inleiding	16
5.2	Relatie tussen de actoren op vlak van het gegevensbeschermingsrecht	16
5.2.1	Verwijzing naar een bestaand rapport	16
5.2.2	Verwerker of leverancier	16
5.3	Koppelen (delen) van politiegegevens.....	17
5.3.1	De Ministeriële richtlijn koppelingen	17
5.3.2	Koppelingen binnen het proces van de politionele cameraverwerkingen	18
5.3.3	De rol van <i>MS Teams</i> bij de koppelingen binnen het proces van de politionele cameraverwerkingen	18
5.3.4	Hybride werken – BYOD – CYOD - COPE	19
5.4	Toegang tot politiegegevens	19
5.4.1	De Ministeriële richtlijn toegangen	19

5.4.2	Toegepast <i>in casu</i> : toegangen binnen een complex systeem van gekoppelde cameraverwerkingen	20
5.5	De risico- en impactanalyses	21
5.5.1	Soorten impact- en risico analyses	21
5.5.2	Een referentie <i>DPIA</i> voor gelijkaardige verwerkingen	21
5.5.3	Toegepast in casu: naar referentie <i>DPIA's</i> voor politionele cameraverwerkingen	21
5.6	Registers	21
5.7	Testen van politionele toepassingen	22
5.8	Didactisch gebruik van camerabeelden	22
6	TOEPASSING VAN DE VASTSTELLINGEN IN DE CASUS EN HET FUNCTIONEEL VIDEOMODEL IN HET LICHT VAN DE VISIE VAN HET COC – SUGGESTIES VOOR TOEKOMSTIGE OPTIMALISATIE BINNEN DE GPI.	22
6.1	Inleiding	22
6.2	Normering van politionele verwerkingen, niet noodzakelijk van politionele gegevensbanken	23
6.3	Keuze voor het bepalen van de juridische relatie tussen (functioneel) verwerkingsverantwoordelijken, verwerker en leverancier	23
6.4	Koppeling van systemen	24
6.5	Beheer van toegangen	24
6.6	Impact- en risicoanalyses – hergebruik van de gegevensbeschermingseffectbeoordeling	25
6.7	Testen van politionele verwerkingen – noodzaak zonder wettelijk kader	25
6.8	Samenvattend	26

1 INLEIDING

1.1 Management Summary

Abstract

In diverse, recent verschenen rapporten heeft het Controleorgaan op de politionele informatie (COC) een visie geponeerd voor een geïntegreerd cameranetwerk binnen de geïntegreerde politie. Politiezones en federale entiteiten kunnen en moeten, onder de wettelijk voorziene omstandigheden, politionele camerabeelden uitwisselen met elkaar. Een concrete casus van samenwerking tussen een federale en lokale entiteit werd nader onderzocht om te kijken welke elementen van de door het COC geponeerde visie reeds in de praktijk konden worden omgezet en op welke hindernissen werd gebotst.

De keuze van het Controleorgaan ligt in dit rapport vooral in het formuleren van suggesties voor optimalisering voor de werking van de GPI¹ *sensu lato* en dus niet in het (bepoort) corrigerend optreden ten aanzien van de bevroegde en bezochte politie-entiteiten.

Keywords

Cameranetwerk – geïntegreerd – *Video Management Systeem (VMS)* – functioneel videomodel – *DPIA* – verwerkingsverantwoordelijke – verwerker – leverancier – MS Teams

¹ Geïntegreerde Politie Police Intégrée

1.2 Kennisname van de feiten

1. Het COC verneemt uit een artikel gepubliceerd in Het Nieuwsblad van 16-05-2022 (stuk 1), dat het *Real Time Intelligence Center (RTIC)* van het SICAD² van de CSD³ Oost Vlaanderen (CSD OVL) rechtstreeks camerabeelden kan bekijken die opgesteld staan op het grondgebied van de PZ Ninove, en dit in het raam van 'een pilootproject'. Het COC kan uit het artikel niet opmaken wie de verwerkingsverantwoordelijke is voor de camera's van de PZ Ninove, noch onder welke regelgeving deze vallen (WPA⁴ dan wel Camerawet), en dus onder welke wettelijke bepalingen het *RTIC* deze beelden verwerkt.

Voorts verneemt het COC dat er, om het opzet van het project te realiseren, heel wat geregeld diende te worden op zowel juridisch als technisch vlak.

2. Artikel Het Nieuwsblad d.d. 16-05-2022:

Pilootproject opgestart waarbij belangrijke informatie meteen bij federale politie terechtkomt Noodcentrale kan live camerabeelden stad bekijken: "Sneller en efficiënter"

De stad Ninove en de federale politie Oost-Vlaanderen zijn begin dit jaar een pilootproject gestart, waarbij de noodcentrale rechtstreeks camerabeelden van tientallen camera's kan bekijken in de stad. Zo kunnen ploegen op het terrein sneller en efficiënter aangestuurd worden bij incidenten.

Ninove is sinds 2015 al gestart met een gefaseerde camera-uitrol. Op die manier wil de stad investeren in de veiligheid van de inwoners. "We hebben ook een eigen regiekamer. Die zorgt ervoor dat we regelmatig zelf camerabeelden kunnen bekijken, en op die manier op het terrein kunnen ingrijpen als dat nodig is", zegt burgemeester Tania De Jonge (Open VLD). Ook het communicatie- en informatiecentrum (CIC) van de federale politie richtte in 2019 een Real Time Intelligence-team (RTI) op. Dat moet ervoor zorgen dat ploegen op het terrein maximaal ondersteund worden, door ze meteen zoveel mogelijk extra informatie te geven tijdens de dispatching.

Bron van informatie

Omdat het cameranetwerk en -systeem van Ninove verschillende raakpunten heeft met dat waarmee het CIC werkt, is er in de loop van 2020 bij beide partijen de bereidheid ontstaan om een pilootproject op te starten, waarbij de Ninoofse camera's ook meteen in het CIC kunnen bekeken worden. Beelden van bewakingscamera's zijn een belangrijke bron van informatie. Wanneer er zich een incident voordoet in een bepaalde straat en iemand de vlucht neemt, dan kunnen camerabeelden een grote hulp zijn. Na een proefperiode heeft het pilootproject al meteen een meerwaarde vertoond in de aanpak van overlastbendes en tussenkomsten bij vechtpartijen. "De politie van Ninove is heel tevreden met de samenwerking", zegt woordvoester van de politiezone Leen Vanhandenhove. "Deze informatiegestuurde manier van werken verhoogd de veiligheid van zowel medewerkers als de burgers."

Niet opgenomen

Concreet kan het team van de noodcentrale beelden consulteren en exploiteren. Camerabeelden kunnen tot drie uur terug opgevraagd worden, maar worden nooit opgenomen. "Als wij bijvoorbeeld een noodoproep binnenkrijgen, kunnen wij meteen de juiste camerabeelden bekijken in Ninove. Op die manier kunnen lokale politieploegen sneller ter plaatse gestuurd worden", zegt Jeroen Duville, diensthoofd van het Real Intelligence-team van de federale politie.

"Het pilootproject zal nu een periode getest worden. Daarna zal bekeken worden of er moet bijgestuurd worden en of er nog andere politiezones kunnen aansluiten bij het project, want criminaliteit stopt niet aan gemeentegrenzen", zegt burgemeester Tania De Jonge. "Momenteel zijn er al contacten met andere Oost-Vlaamse politiezones om het project

² Communicatie- en informatiedienst van het arrondissement, bestaande uit de pijler CIC en de pijler AIK. Het CIC staat voor Communicatie en Informatie Centrum. En staat in voor het *real time* gebeuren via de calltaking en de dispatching van de ploegen op het terrein. Het AIK is de tweede pijler van deze SICAD-werking en staat in voor de verwerking van de informatie in tweede lijn.

³ Coördinatie- en steundienst in de zin van de Wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus (WGP) en de Wet van 5 augustus 1992 op het politieambt (WPA).

⁴ Wet van 5 augustus 1992 op het politieambt.

uit te breiden. Zowel op juridisch als technisch vlak moest er heel wat geregeld worden, maar we zijn ontzettend trots op de realisatie en kijken uit naar een verdere uitbreiding binnen de provincie”, besluit Jeroen Duville.”

2 TER HERINNERING – DE VISIE VAN HET COC

3. De door het COC geponeerde visie⁵ omtrent geïntegreerde cameraverwerkingen binnen de GPI luidt als volgt. Het NIP⁶, als nationale component van de GPI, de 10 meldkamers van de provinciale CIC⁷ als gedeconcentreerde component van de GPI, alsmede de dienst Luchtsteun (DAFA) van de federale politie en vele dispatchings van lokale politiezones beschikken over een zgn. ‘*Video Management System*’ (VMS), die het *real time* bekijken van beelden alsmede de opslag en verdere verwerking toelaat.

De federale VMS systemen, zijnde deze van het NIP, van de meldkamers van de CIC en van de dienst Luchtsteun zijn al onderling met elkaar verbonden om de beelden van de helikopters en/of de *drones* van de dienst DAFA, die middels 8 masten gecaptureerd en doorgestuurd worden naar de VMS van DAFA, te kunnen ontvangen. Aldus vormt dit systeem alsmede de deelnemende VMS systemen reeds *de facto* een *backbone* voor wat verder nationaal zou kunnen uitgerold worden. Deze *backbone*, gekoppeld aan de nationale en regionale glasvezelnetwerken die, dankzij de uitrol van het nationaal ANPR netwerk, werden geconnecteerd met het Datacenter van de GPI, kunnen aldus gebruikt worden om zowel politionele (WPA) als camera’s van derde partijen (Camerawet), tot eventueel zelfs op termijn *videocalls* van burgers, te ontvangen en verder te ontsluiten.

Een videomanagementsysteem, ook bekend als *videomanagementsoftware* of een *videomanagementserver*, is een onderdeel van een beveiligingscamerasysteem dat in het algemeen:

- de beelden van camera's en andere bronnen verzamelt;
- de beelden opslaat;
- een *interface* biedt om zowel de *live* video te bekijken als toegang te krijgen tot de opgeslagen beelden.

Door de verbeteringen in de technologie is het noodzakelijk een onderscheid te maken tussen een *Video Management System* (VMS) en de ingebouwde functies van moderne, netwerk gebaseerde, beveiligingscamera's. Veel moderne netwerkcamera's bieden interne mogelijkheden om zelf rechtstreeks videobeelden op te nemen en te bekijken via een webbrowser en zonder gebruik te maken van een VMS. Ook voor *drone*-camera's bestaan deze mogelijkheden, gaande van de opslag op de SD kaart tot het *streamen* van de beelden. Voor een **geïntegreerde** aanpak van politioneel cameragebruik is een VMS dus noodzakelijk.

4. Een VMS staat ook in verband met een efficiënt en geïntegreerd management van het cameragebruik. Als de verschillende bestaande VMS'en binnen de GPI zich in één videobewakingssysteem integreren en federeren, met een geconsolideerde juridische status, alsmede zijn eigen functioneel videomodel, wordt de videosynergie van de binnen de GPI gebruikte cameratypes, alsmede tussen de GPI en haar externe partners, aanzienlijk vergemakkelijkt: standaardovereenkomsten en protocolakkoorden, model DPIA's en één technische aansluiting zouden dan volstaan om de uitwisseling van camerabeelden te verwezenlijken. Aldus zouden zij een toegangspoort vormen voor camerabeelden die politioneel kunnen gebruikt worden, wat enerzijds een risico zou kunnen vormen indien niet de gepaste mitigerende maatregelen worden genomen, maar anderzijds aanzienlijk wat voordelen biedt voor een kwalitatiever gegevensbeheer en een verminderd potentieel voor misbruik van gegevens; een uniform veiligheidsbeleid zou kunnen toegepast worden waarbij sterke garanties naar traceerbaarheid en vertrouwelijkheid van gegevens geboden kunnen worden, wat het operationele politionele cameragebruik alleen maar ten goede kan komen.

⁵ CON20004 en DIO20009 (openbaar gepubliceerd); DIO23004 (enkel intern GPI beschikbaar).

⁶ Nationaal InvalsPunt.

⁷ CIC staat voor Communicatie en Informatie Centrum. Het is de eerste pijler van de provinciale SICAD werking, die instaat voor het *real time* gebeuren via de *calltaking* en de dispatching van de ploegen op het terrein. Het AIK is de tweede pijler van de SICAD werking; deze staat in voor de verwerking van de informatie in tweede lijn.

3 OPZET VAN HET TOEZICHT EN METHODOLOGIE

5. In het licht van de door het COC geponeerde visie voor een geïntegreerd cameranetwerk binnen de geïntegreerde politie werd naar aanleiding van het voornoemde artikel op 19-05-2022 door het DIRCOM COC een toezichtonderzoek opgestart met de opdracht aan de dienst onderzoeken van het COC (DOSE) om de DirCo⁸ OVL te bevragen naar (stuk 2):

- 1) Alle voorhanden zijnde stukken betreffende:
 - het pilootproject op zich met de PZ Ninove;
 - de uitbouw van het RTIC bij het SICAD OVL.
- 2) Welke juridische en technische zaken kennelijk nog moeten geregeld worden inzake het pilootproject.

6. In navolging van de opdracht van het DIRCOM COC en teneinde te kunnen overgaan tot een *prima facie* analyse werden op 23-05-2022 de volgende stukken bij de DirCo OVL opgevraagd (stuk 3):

- 1) betreffende het pilootproject camera's Ninove:
 - de rechtsbasis van deze cameraverwerkingen: camerawet, WPA,...;
 - of er al dan niet een DPIA⁹ werd gemaakt en zo ja, een kopie van deze DPIA;
 - projectfiches, presentaties, functionele, technische en processchema's waaruit het concept van het opzet blijkt (*high level*);
 - dienstnota's en interne richtlijnen specifiek met betrekking tot deze cameraverwerkingen;
- 2) betreffende de uitbouw van het RTIC in het SICAD:
 - dienstnota's, interne richtlijnen over de werking van het RTIC;
 - presentaties over deze werking.

7. De DirCo OVL gaf te kennen in zijn ontvangstmelding van 23-05-2023, dat heel wat documentatie door de PZ Ninove wordt beheerd, en dat hij dientengevolge in overleg met hen alle gevraagde documentatie zal verzamelen en bezorgen (stuk 4).

8. Ingevolge de vraagstelling van het COC bleek één en ander geactualiseerd te moeten worden bij beide politie-entiteiten (stuk 5). Op 10-08-2022 bezorgde de DirCo OVL een aantal stukken via mail (stuk 6):

- de DPIA PZ Ninove – CSD: uitgevoerd door de DPO PZ Ninove en DPO CSD OVL en geactualiseerd op 08-08-2022 (stuk 7);
- de DPIA PZ Ninove – CSD: uitgevoerd op 22-02-2021 (oude versie die nu geactualiseerd werd) (stuk 8);
- het privacy protocol PZ Ninove – CSD OVL van 07-07-2022 getekend door de DirCo, ondertekening door de KC is voorzien zodra het mogelijk is (stuk 9);
- de werkingsregels PZ Ninove (zoals gepubliceerd op sharepoint) (stuk 10);
- de werkingsregels Team RTI CIC OVL (zoals gepubliceerd op sharepoint) (stuk 11).

De DirCo OVL nodigde het COC tevens uit voor een plaatsbezoek zodat de werking in *real time* kan bekeken en toegelicht worden. Het COC repliceerde hierop, dat de nodige analyses zullen worden uitgevoerd en dat de DirCo op de hoogte zal worden gehouden (stuk 12).

9. Uit de analyse van de stukken blijkt, dat er naast juridische ook heel wat technische vragen te stellen zijn.

10. Evenwel is van bij de eerste analyse van de stukken duidelijk, dat de applicatie *MS Teams* van het O365 pakket van Microsoft, zoals in gebruik bij de GPI, een rol speelt bij het uitwisselen van beelden tussen het RTIC en de PZ Ninove. Aldus stelt het COC op 18-08-2022 een aantal vragen inzake de rol van *MS Teams* bij de cameraverwerkingen van de GPI aan andere politie-entiteiten:

⁸ De arrondissementele bestuurlijke directeur-coördinator van de federale politie in de zin van de Wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus (WGP) en de Wet van 5 augustus 1992 op het politieambt (WPA).

⁹ *Data Protection Impact Assessment*, of gegevensbeschermingseffectbeoordeling

- 1) de dienst DGA/DAS¹⁰ (stuk 13);
- 2) de dienst DGA/DAFA¹¹ (stuk 14);
- 3) de dienst DGR/DRI¹² (stuk 15).

11. Op 18-08-2022 antwoordt de dienst DGA/DAS, dat zij geen gebruik maken van de applicatie *MS Teams* maar wel een alternatieve communicatie hebben met een eigen server (stuk 16).

12. Op 19-08-2022 krijgt het COC kennis van een concept "Videoplatform GPI" met ook een rol voor *MS Teams* (stuk 17). Dit sluit aan bij de visie van de DPO van DGA/DAS 08-09-2022, waarbij werd gesteld toch interesse te hebben voor het gebruik van *MS Teams* daar deze een meerwaarde zou kunnen bieden (stuk 21).

13. Op 22-08-2022 antwoordt DGR/DRI (stuk 18). Als bijlage voegt DGR/DRI tevens een korpsnota DRI 2019/5304 *Gebruikersgids 'police cloud' oplossingen (Microsoft 365) binnen de Geïntegreerde Politie* d.d. 11-06-2019 (stuk 19) toe.

14. Op 12-09-2022 antwoordt DGA/DAFA (stuk 20). DAFA heeft al een paar keer gebruik gemaakt van *MS Teams*. Op 23-09-2022 geeft DGA/DAFA concreet aan hoe dit gebeurt (stuk 22).

15. Verdere interne analyses resulteren in het opstellen van een vragenlijst voorafgaand aan een plaatsbezoek aan het SICAD/CIC/RTIC OVL en de PZ Ninove. Op 23-11-2023 wordt de vragenlijst overgemaakt aan beide verwerkingsverantwoordelijken (stuk 23).

16. Op 27-11-2023 antwoordt de DirCo OVL dat de antwoordelementen gezamenlijk zullen worden opgesteld (stuk 24). Tevens stelt hij februari 2024 voorop als datum voor een plaatsbezoek aan beide politie-entiteiten.

17. Op 05-02-2024 ontvangt het COC de antwoordelementen op de op 23-11-2023 gestelde vragen (stuk 25).

18. De plaatsbezoeken vinden plaats te Gent op 30-04-2024 om 10:00 (stukken 30 en 33), en te Ninove op 30-04-2024 om 13:00 (stukken 29 en 33).

19.1. Op 18-08-2025 wordt het ontwerp rapport in prelectuur en op tegenspraak overgemaakt aan de korpschef PZ Ninove en de DirCo OVL (stuk 34).

19.2. Op 08-09-2025 wordt door de DIRCO OVL aan het COC geantwoord dat er geen aanvullingen of vragen bij het ontwerp van verslag zijn van zijn kant en wordt nog meegegeven dat, na publicatie van het definitieve verslag, er door de DIRCO OVL met de KC PZ Ninove en de DPO PZ Ninove zal worden bekeken welke werkpunten kunnen geredigeerd worden op hun niveau maar dat tegelijk ook de samenwerking rond de camerabeelden quasi stil ligt aangezien het CIC OVL momenteel over geen capaciteit RTI beschikt (stuk 35).

19.3. Op 12-09-2025 wordt door de korpschef PZ Ninove aan het COC geantwoord dat hij geen aanvullingen of vragen heeft naar aanleiding van dit rapport. Samen met de DPO Dender Schelde en CSD Oost-Vlaanderen zal de PZ Ninove de gesuggereerde werkpunten bekijken teneinde na te gaan wat er kan aanpast worden op hun niveau. Bijkomend geeft de korpschef PZ Ninove mee dat het project RTI slapend is geworden daar de CSD Oost-Vlaanderen geen capaciteit heeft om het RTI te bemannen. Tevens wijst de korpschef PZ Ninove op het feit dat de PZ Ninove vanaf oktober 2025 overgaat naar een 24/7 permanentie in het politiehuis waardoor de PZ Ninove ook voor cameratoezicht minder steun nodig zal hebben vanuit de CSD (stuk 36).

¹⁰ De Directie openbare veiligheid (DAS) is de gecentraliseerde steuneenheid die als onderdeel van DGA aan alle entiteiten van de GPI, verschillende vormen van steun verstrekt in het kader van het genegotieerd beheer van de publieke ruimte, in het bijzonder ploegen en middelen gespecialiseerd in preventie en oplossing van gewelddadige of gevaarlijke situaties.

¹¹ De Dienst Luchtsteun (DAFA) is een gespecialiseerde politiedienst die de Federale en Lokale Politie bijstaat vanuit de lucht om een betere en efficiëntere politiezorg te verzorgen. De luchtmiddelen worden ingezet enerzijds voor het verzamelen van (politie) informatie en anderzijds als interventie-middel (bijvoorbeeld waterdropping).

¹² De Directie van politie-informatie en ICT-middelen (DGR/DRI) is verantwoordelijk voor het concept van politie-informatie, de voorbereiding van informatieverwerking en communicatiesystemen, de technische normen, de processen van de arrondissementale informatie- en communicatiediensten, het beheer van de ANG, de operationele documentatie, enz.

4 ONDERZOEKSBEVINDINGEN

4.1 Inleiding

20. De aangeleverde stukken verwijzen soms naar niet van toepassing zijnde regelgeving zoals de AVG, of naar niet tot de *scope* van het toezichtonderzoek behorende cameraverwerkingen zoals *ANPR* of niet-zichtbaar politieel cameragebruik. Een hoofdstuk over toepasselijke normen stelt, dat deze er niet zijn. Herhaaldelijke verwijzingen naar stadscamera's doen vermoeden dat de politie niet de exclusieve gebruiker is van de camera's. Sommige stukken zoals de gezamenlijke *DPIA* (stuk 7) alsmede het privacy-protocol (stuk 9) dateren van **nà** de vraagstelling door het COC of werden naar aanleiding daarvan geactualiseerd, respectievelijk 08-08-2022 en 07-07-2022. Bepaalde onderwerpen worden eerder zeer algemeen aangeraakt en niet verder uitgewerkt. Zo levert een zoeking op de aan- of afwezigheid in de tekst van de - nochtans verplichte¹³ – MFA¹⁴ geen enkel resultaat op. Geen van de aangeleverde stukken lijkt rekening te houden met de in art 44/4 WPA voorziene Ministeriële dwingende richtlijnen inzake informatieveiligheid¹⁵, de toegangen¹⁶ of de koppelingen¹⁷.

Gegeven de talrijke onduidelijkheden worden uit 59 initiële vragen en opmerkingen van het COC verdere vragen geclusterd en overgemaakt aan de entiteiten PZ Ninove en CSD OVL (stuk 23) voor hetzij gezamenlijk, dan wel apart per entiteit te beantwoorden, of locaties dan wel handelingen te tonen tijdens de aangekondigde plaatsbezoeken (stukken 29 en 30).

21. De thematisch geclusterde vragen en opmerkingen worden hieronder nader toegelicht en aangevuld met de antwoordelementen van de entiteiten PZ Ninove en CSD OVL (stuk 25), andere bevroegde entiteiten (stukken 16, 18, 19, 20, 21), documentatie over het functioneel videomodel GPI (stuk 17) alsmede de vaststellingen van de plaatsbezoeken (stukken 29 en 30).

4.2 Verhouding tussen de betrokken actoren

4.2.1 PZ Ninove en CSD OVL

22. Na lezing en analyse van de *DPIA's* (stukken 7 en 8) is het voor het COC niet duidelijk hoe de entiteiten PZ Ninove en de CSD OVL zich t.a.v. elkaar verhouden, noch vanuit welk perspectief het document geschreven is. Het COC vraagt zich af of het gaat om een concept van 'gezamenlijke verwerkingsverantwoordelijken' zoals bepaald in artikel 52 WVG, dan wel of is er sprake van een relatie van 'verwerkingsverantwoordelijke – verwerker' conform artikel 53 WVG. Dergelijke keuze van relatie tussen beide actoren heeft immers een invloed op daaruit voortvloeiende protocollen voor afspraken met betrekking tot verplichtingen, o.a. inzake het uitoefenen van het recht op inzage, op basis van welke rechtsgronden er wordt gewerkt, enz. ... (stuk 23). Hieromtrent stelt het gezamenlijk antwoord van beide politie-entiteiten het volgende (stuk 25) (letterlijke weergave):

"De DPIA over PZ Ninove (CSD OVL) gebruik camerabeelden werd opgesteld door (...), zonder dat deze DPIA werd meegedeeld aan de DPO Dender-Schelde en dus ook zonder akkoord van de DPO Dender-Schelde.

De DPIA die d.d. 8 augustus 2022 werd opgesteld tussen de politiezone Ninove en CSD OVL – SICAD betreft een verduidelijking bij de rolbepaling binnen deze DPIA.

De korpschef van de politiezone Ninove is de verwerkingsverantwoordelijke voor de cameraverwerkingen binnen de politiezone Ninove.

¹³ Gemeenschappelijke bindende richtlijn van de Ministers van Justitie en van Binnenlandse Zaken van 13 juli 2021 met betrekking tot de toegangsregels van de leden van de politiediensten tot de algemene nationale gegevensbank en de basis-, bijzondere en technische gegevensbank.

¹⁴ Authenticatie gebaseerd op verschillende factoren of "Multi-Factor Authentication". Is gebaseerd op ten minste twee van de volgende drie elementen: een element "kennis" (iets dat alleen de gebruiker weet), een element "bezit" (iets dat alleen de ondertekenaar heeft) en een element "hoedanigheid" (iets dat de gebruiker is).

¹⁵ Art. 44/4 §2 WPA.

¹⁶ Art. 44/4 §3 WPA.

¹⁷ Art. 44/4 §4 WPA.

De DirCo van Oost-Vlaanderen is op zijn beurt de verwerkingsverantwoordelijke voor de opdrachten van bestuurlijke en gerechtelijke politie wanneer hij ploegen van CSD Oost-Vlaanderen aanstuurt".

Daarnaast stellen de politie-entiteiten te kunnen afleiden uit correspondentie met het COC, dat het COC de DirCo OVL beschouwt als enige verwerkingsverantwoordelijke. Daarbij lijkt inzonderheid de *DPO* Dender Schelde, zijnde de *DPO* voor de PZ Ninove, er, ten onrechte, van uit te gaan dat er klaarblijkelijk aparte besprekingen hebben plaatsgevonden tussen de DirCo OVL en het COC, vermits deze stelt:

"De DPO van politiezone Dender-Schelde werd nooit op de hoogte gebracht van de inhoud van deze bespreking(en) en eventuele noodzakelijke aanpassingen". (letterlijke weergave):

Beide politie-entiteiten werden evenwel transparant van elke communicatie vanwege het COC als bestemming geplaatst.

4.2.2 DGR/DRI en *Microsoft* als verwerkers

23. Initieel maken de entiteiten PZ Ninove en CSD OVL gewag van *Microsoft* en DRI als zijnde verwerkers (stukken 7 en 8). Hieromtrent bevraagd (stuk 23), stellen de beide politie-entiteiten het volgende (stuk 25) (letterlijke weergave):

"Binnen deze verwerking - politionele camerabewaking op een niet-besloten plaats en RTI door CSD Oost-Vlaanderen - wordt er gebruik gemaakt van het toegangsbeleid GPI, onder algemeen beheer van DRI, tot de office 365 omgeving, specifiek Microsoft Teams, voor de doorgifte van screenshots van beelden tussen CSD Oost-Vlaanderen en de operationele medewerkers van de PZ Ninove met toegangsrechten tot het specifieke kanaal in Microsoft Teams.

DRI is de verwerkingsverantwoordelijke voor het Microsoft 365-pakket en is dusdanig een betrokken partij aangezien men de camerabeelden via Teams deelt. De keuze van 'verwerker' in DPIA versie 1.0 was geen doordachte keuze aangezien er geen specifieke verwerkingen plaatsvinden door de betrokken partijen".

24. De nota DRI 2019/5304 (stuk 19) vermeldt hieromtrent evenwel (letterlijke weergave):

"Elk lid van de GPI die gebruiker is van de oplossingen die hem/haar ter beschikking worden gesteld, draagt hiervoor de verantwoordelijkheid. Hij/zij moet dus het wettelijk en professioneel kader naleven, naargelang zijn/haar eenheid en rol.

Elke eigenaar (owner) van een groep (bv. de eigenaar van een team in Yammer, Teams, SharePoint-site, ...) die in het systeem voorkomt, is verantwoordelijk voor alle informatie die binnen de groep wordt beheerd én voor het beheer zelf van de groepsleden. Hij moet ervoor zorgen dat de verschillende regels inzake informatieuitwisseling worden nageleefd (geheim van het onderzoek, beroepsgeheim, bescherming van persoonsgegevens enz.).

De diensthouders dragen een functionele managementverantwoordelijkheid, identiek aan hun verantwoordelijkheid voor alle systemen die hun medewerkers gebruiken".

25. De gezamenlijke *DPIA* (stuk 7) stelt tevens geen gebruik te maken van externe *cloud providers*. Nochtans wordt het Microsoft O365 GPI pakket omschreven als zijnde een *cloud*-oplossing, met inzonderheid in dit dossier een bijzondere rol voor *MS Teams*.

4.2.3 Tein, Genetec en Edesix als verwerkers

26. Initieel maken de entiteiten PZ Ninove en CSD OVL gewag van Tein, Edesix (PZ Ninove) en Genetec (CSD OVL) (stukken 7 en 8) hetzij tekstueel, hetzij in de vorm van schema's. Hieromtrent bevraagd (stuk 23) stellen de beide politie-entiteiten het volgende (stuk 25) (letterlijke weergave):

"Het onderhoud om inbraakveilig te zijn gebeurt door de verwerker. Tein levert soft- en hardware en support aan de verwerker. Genetec Inc. is de leverancier van software aan de subverwerker. Het Genetec Security Center zorgt voor de software voor de camera's. De software voor de bodycams (Edesix) valt buiten de scope van RTI".

27. Geen van de aangeleverde stukken wijst op een actieve en door de verwerkingsverantwoordelijken opgelegde verwerking van persoonsgegevens door de private entiteiten Tein, Edesix of Genetec. In stuk 10 lijkt een rol te zijn weggelegd voor Tein wat betreft incident management:

"Indien het een nieuw defect betreft zal door PZ Ninove asap contact opgenomen worden met Tein".

Ook uit de plaatsbezoeken kon niet afgeleid worden, dat een of meerdere van de genoemde private entiteiten actief persoonsgegevens verwerkt voor een van de entiteiten GPI als (functioneel) verwerkingsverantwoordelijke. Wel blijkt uit de plaatsbezoeken dat aan Tein een rol toebedeeld wordt inzake de creatie van gebruikers van de VMS systemen in de PZ Ninove (stuk 29). De gebruikers CSD OVL daarentegen worden aangemaakt door DGR/DRI (stuk 30). Ook beheert Tein de firewall (stuk 29).

28. Uit het gezamenlijk antwoord van beide politie-entiteiten (stuk 25) blijkt verder, dat er een verwerkingsovereenkomst is tussen Tein en de PZ Ninove, en tussen Genetec en DGR/DRI.

4.3 Scope van het project

29. Gegeven het geïntegreerde en integrale karakter van de geponeerde visie van het COC stelt het COC tevens vragen aan beide politie-entiteiten inzake de *scope* van het project op het vlak van heli- en *drone*beelden, maar evengoed op het vlak van beelden gemaakt door een individuele camera, beelden verwerkt onder art 112ter Sv (audiovisuele opname van een verhoor op vordering van de procureur des Konings), alsmede beelden afkomstig van vaste bewakingscamera's van een derde partij gelegen op het grondgebied van de PZ Ninove, zoals bijvoorbeeld de stad of Infrabel. Daarnaast wordt ook de vraag gesteld of de controle op de naleving van de arbeidsvoorwaarden¹⁸ gerekend wordt tot de *scope* van het project (stuk 23). Tevens worden vragen gesteld inzake de rol van CAD¹⁹ (zie punt 4.5) en ISLP²⁰ (zie punt 4.6).

30. Omtrent de genoemde verwerkingen stelt het gezamenlijk antwoord van beide politie-entiteiten, dat beelden van de camera's van de helikopter, van *drones*, alsmede van individuele camera's en verhoorcamera's buiten *scope* zijn (stuk 25). Volgende argumenten worden daarbij aangehaald:

- het in *real time* bekijken van helibeelden wordt door de Federale Politie gedaan; achteraf kunnen relevante en opgeslagen beelden opgevraagd en in beslag worden genomen;
- het zou overmatig van aard zijn om de PZ Ninove nationale beelden te laten exploiteren;
- geen van de genoemde politie-entiteiten beschikt over *drones*;
- de individuele camera's van de PZ Ninove laten geen livestream toe; indien de FGP²¹ van OVL beelden wenst kunnen deze geraadpleegd of gedeeld worden op basis van een kantschrift;
- de beelden van de audiovisuele verhoren²² worden op een aparte server bewaard, weggeschreven op externe gegevensdragers en vervolgens gewist op de server;
- de camera's waarvan sprake zijn de eigendom van de stad Ninove, doch de PZ Ninove is de exclusieve gebruiker en de verwerkingsverantwoordelijke;

¹⁸ Zie Advies uit eigen beweging BD200007 dd 17-08-2020 met betrekking tot het invoeren van camerabewaking door de geïntegreerde politie met het oog op de controle van de naleving van de arbeidsvoorwaarden.

¹⁹ Computer Aided Dispatching is een gemeenschappelijke benaming voor het geheel van de toepassingen die worden gebruikt met het oog op het implementeren van een computerondersteunde meldkamer. De CAD-omgeving bestaat uit verscheidene hardware- en softwareonderdelen. Het COC beschouwt dit als een basisgegevensbank in de zin van art 44/11/2 WPA.

²⁰ Integrated System for Local Police. Basisgegevensbank in de zin van art 44/11/2 WPA.

²¹ Federale Gerechtelijke Politie

²² Dit cameragebruik valt voor alle duidelijkheid niet onder de regeling van het cameragebruik bedoeld in de WPA.

- technisch zit het delen van helibeelden, *drone*beelden, beelden van individuele camera's, beelden van de verhoorcamera's van de PZ Ninove of beelden van het commissariaat van de PZ Ninove niet in de *scope* van het project.

Bovendien stellen de politie-entiteiten dat het gebruik van de beelden voor de controle op het naleven van de arbeidsvoorwaarden niet onder de *scope* van het project valt. Nochtans maakt de gezamenlijke *DPIA* (stuk 7) hierop een allusie door te stellen (letterlijke weergave):

"Indien de camerabewaking (ook) betrekking of impact heeft op de werkomstandigheden en arbeidsprestaties van het personeel van de politiediensten is (ook) de AVG en de WGB van toepassing (Aanbeveling GBA 06/2011) De diverse camera's van de politiezone zijn geregistreerd in het beeldverwerkingsregister".

"De diverse doelstellingen (bestuurlijk, gerechtelijk of personeelsbeheer) zijn tevens vervat in dit register en ter kennis gebracht aan het BOC".

Uiteindelijk wordt de *scope* omschreven als volgt (stuk 25):

"De cyclus start bij de toezichtcamera's die zich bevinden op het grondgebied van de Stad Ninove. De diverse camerasystemen worden beheerd in het globaal video management system (VMS). CSD OVL – RTI heeft via een Firewall VPN realtime toegang tot de beelden en kan tot maximum 3 uren terugkijken. CSD OVL – RTI ondersteunt de interventieploegen van PZ Ninove doormiddel van het delen van beelden of korte fragmenten in het daarvoor bestemde Teamskanaal. De cyclus eindigt dus bij PZ Ninove die de beelden kan bekijken in het Teamskanaal".

4.4 Rol van *MS Teams*

4.4.1 Algemeen

31. Gegeven de summiere omschrijving van de rol van *MS Teams* bij de werkprocessen in de stukken 7, 8 en 11 bevraagt het COC de beide politie-entiteiten omtrent de rol van *MS Teams* (stuk 23). Het gezamenlijke antwoord van beide politie-entiteiten luidt als volgt (stuk 25) (letterlijke weergave):

"Teams is onderdeel van het Microsoft 365-pakket".

De cyclus omschreven in stuk 25 en hierboven geciteerd geeft iets meer duidelijkheid. Het volledige proces wordt exhaustief toegelicht door beide politie-entiteiten naar aanleiding van het plaatsbezoek op 30-04-2024.

4.4.2 Traceerbaarheid en logging *MS Teams*

32. Inzake de traceerbaarheid en de logging van de verwerkingen in het *MS Teams* kanaal stelt het gezamenlijk antwoord van beide politie-entiteiten het volgende (stuk 25) (letterlijke weergave):

"Iedereen met toegang tot het Teamskanaal kan dit bekijken. Momenteel is het onmogelijk te traceren welk personeelslid een bepaald camerabeeld heeft geraadpleegd in Teams. De politiezone Ninove zal met DRI nagaan of er mogelijkheden zijn om die tracersing mogelijk te maken".

4.4.3 Controle op verdere verspreiding

33. Gegeven de mogelijkheid om vanuit *MS Teams* gegevens te downloaden en bij ontstentenis van een beleid hieromtrent in de aangeleverde stukken 7, 8 en 11 stelt het COC de vraag hoe de controle verloopt op een eventuele verdere verspreiding van zodra de *MS Teams* omgeving wordt verlaten (stuk 23). Het gezamenlijk antwoord van beide politie-entiteiten luidt als volgt (letterlijke weergave):

"Er gebeurt geen periodieke controle, maar er vinden controles plaats indien de dienst Intern toezicht de politiezone Ninove op de hoogte brengt van bepaalde incidenten.

De deontologische code is van toepassing".

4.4.4 Beleid rond mobiele toestellen waarop *MS Teams* geïnstalleerd is

34. Gegeven de mogelijkheid tot gebruik van *MS Teams* op allerlei mobiele toestellen stelt DOSE een aantal vragen rond BYOD²³ voor professioneel gebruik, het privégebruik van diensttoestellen alsmede het gemengd gebruik door derden in hoofdzaak familieleden van, hetzij BYOD toestellen, hetzij professionele toestellen (stuk 23). Het gezamenlijk antwoord van beide politie-entiteiten luidt als volgt (stuk 25) (letterlijke weergave):

"De politiezone Ninove beschikt niet over mobiele persoonlijke devices, maar enkel over tablets die in de zone blijven of bij wachtdiensten mee naar huis worden genomen en enkel voor professionele doeleinden kunnen worden gebruikt. Mensen gebruiken op eigen initiatief teams op hun persoonlijk toestel.

De politiezone Ninove stelde een policy op betreffende internet en het gebruik van mobile devices.

CSD Oost-Vlaanderen beschikt over een policy voor het beheer van Teamsgroepen, desktop/laptop en smartphones. Wat betreft die laatste twee devices is de situatie zowel geregeld als het gaat over privétoestellen als over toestellen die door de directie worden aangekocht. Deze policy is gepubliceerd op een Sharepointsite en is toegankelijk voor alle personeelsleden van CSD Oost-Vlaanderen".

4.4.5 Alternatieven voor *MS Teams*

35. Gevraagd naar andere technologieën voor verspreiden van beelden dan *MS Teams* (stuk 23) waarbij onder andere gerefereerd wordt aan *Astrid Picture Push*²⁴ alsmede aan toegangspunten met mobiele (telefoon)data-abonnementen, stellen de politie-entiteiten in hun gezamenlijk antwoord (stuk 25) (letterlijke weergave):

"Dat is niet gekend bij PZ Ninove.

CSD Oost-Vlaanderen gebruikt dit niet omdat men controle wil houden op de aangeleverde informatie aangezien er anders geen ventilatie plaatsvindt".

36. De dienst DGA/DAS lijkt voor beeldverspreiding over een eigen oplossing te beschikken (stuk 16) (letterlijke weergave):

"Binnen DAS maken wij geen gebruik van de toepassing Teams om beelden te versturen.

De reden hiervoor is dat het meestal te grote bestanden betreft (meerdere gigabytes). Onze eenheid beschikt over toestellen die beelden kunnen maken in 4K. Dit komt de beeldkwaliteit ten goede maar heeft als consequentie dat de bestanden groter zijn.

DAS beschikt over een server waarop de beelden geplaatst worden.

Softwarematig wordt een unieke link gemaakt per file, die moet worden overgedragen. Deze link wordt gekoppeld aan een paswoord. Vervolgens wordt de link met het paswoord via de politiemail overgemaakt aan de bestemming van de beelden.

Door op de link te klikken wordt de ontvanger van de beelden rechtstreeks naar onze server geleid, waarbij de beelden vervolgens door de partner kunnen worden gedownload.

We beschikken eveneens over de mogelijkheid om de download te beperken in tijd, of het aantal keer dat de file kan worden gedownload. Indien we spreken over 10-tallen gigabytes gaan we over tot het overzetten van de beelden op een draagbare gegevensdrager of we vragen aan de entiteit om met een laptop rechtstreeks tot bij ons langs te komen voor de overdracht".

Uit een repliek van de DPO DGA/DAS omtrent dezelfde verwerking blijkt evenwel de interesse voor *MS Teams*, al heeft de bevrageerde DPO een aantal twijfels (stuk 21) (letterlijke weergave):

²³ Bring Your Own Device: de medewerker gebruikt op vrijwillige basis zijn eigen apparaten. De beveiliging is niet uniform, hangt af van de gebruiker en is daardoor vaak minder goed verzekerd; het apparaat wordt ook privé gebruikt en het apparaatmanagement is complex(er) voor de organisatie..

²⁴ Picture Push is een functie die eigen is aan de ASTRID Mobile Data Connectivity Server (MDCS) en die de mogelijkheid biedt om foto's te sturen naar mobiele terminals. Voorlopig kunnen enkel foto's gestuurd worden naar TETRA radio's, maar later zal dit ook kunnen naar mobiele eindapparaten (tablets, laptops, smartphones,...) die uitgerust zijn met een Blue Light Mobile (BLM) SIM-kaart.

"Deze applicatie werd reeds aan een test onderworpen en zou een meerwaarde kunnen bieden in operationele livesituaties. Wij menen bovendien op de veiligheid van door DRI aangeboden applicaties te mogen rekenen.

In afwachting van uw eventuele standpunt lijkt het ons dan ook niet aangeraden het gebruik ervan al dan niet toe te staan".

37. Het functioneel videomodel van de GPI (stuk 17) voorziet, naast een koppeling tussen verschillende VMS in verschillende politie-entiteiten, met inzonderheid een rol voor de SICAD/CIC, ook een rol voor *MS Teams*, al lijkt deze rol zich te beperken tot het in *real time* bekijken van beelden, mits schermdeling met een operator van de dienst DGA/DAFA. De reactie van DGA/DAFA lijkt dit te bevestigen (stuk 20) (letterlijke weergave):

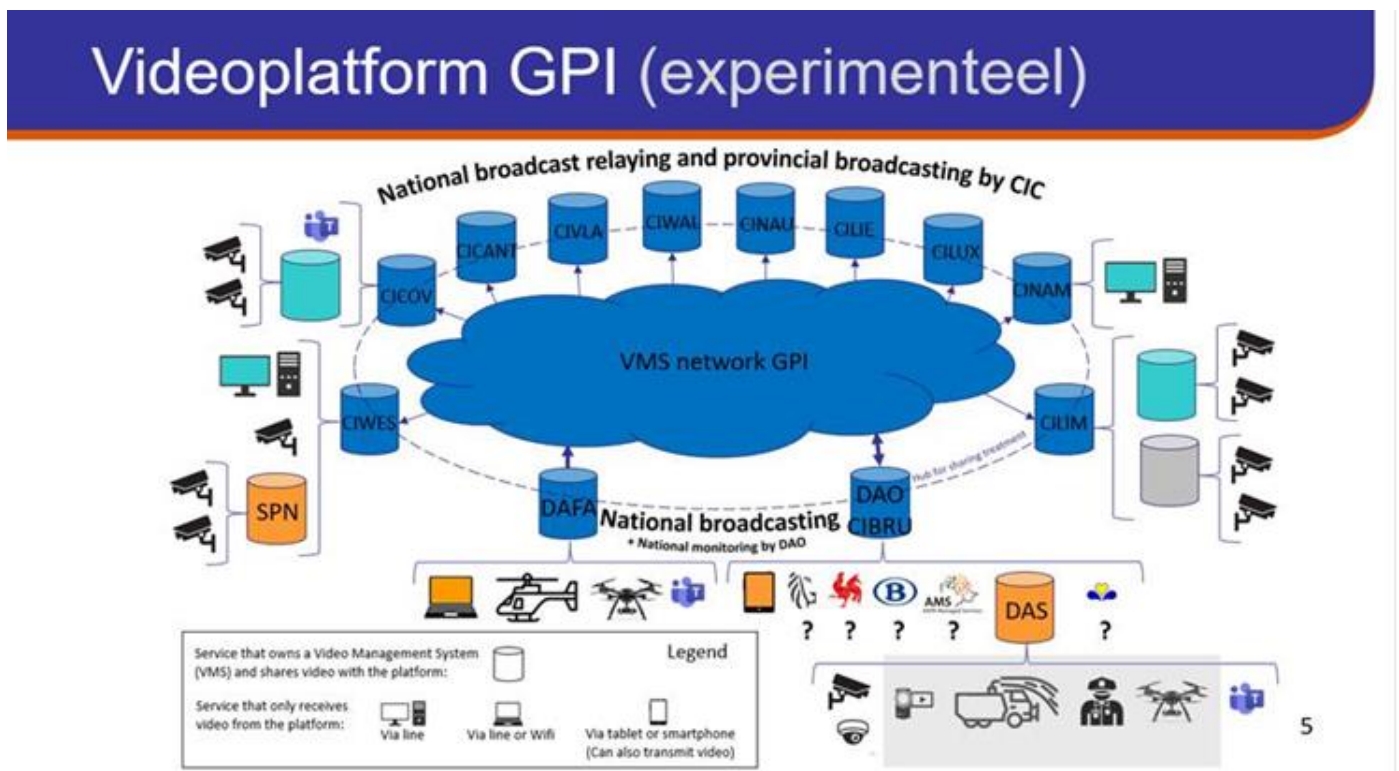
"DAFA heeft al een paar keer gebruik gemaakt van teams om beelden door te stralen op momenten dat wij problemen vaststelden met de beelddoorstraling.

Bij het gebruik in het verleden werd er altijd doorgestraald naar een collega van de geïntegreerde politie, niet naar externer".

Dit wordt nog verder toegelicht (stuk 22):

"De beelden komen binnen op de server van DAFA. Via de PC die de server beheert starten we een teams sessie met "de klant". Het scherm wordt gedeeld zodat de beelden zichtbaar worden".

Een tekening van het conceptuele videomodel ziet eruit als volgt (stuk 17):



Dit model wordt verder toegelicht (stuk 17), en kan geparafraseerd als volgt worden geduid:

- 1) het model is gericht op zowel het ontvangen van beelden als het verspreiden van beelden, van eender welke camera-sensor waarvoor een wettelijke basis bestaat voor politieeel gebruik;
- 2) DAFA en DAO verspreiden de beelden van nationaal belang naar de SICAD/CIC. Het gaat om beelden:
 - van de camera van de helikopter DGA/DAFA;
 - van de camera's van de *drones* van eender welke politie-entiteit en voor zover voorzien van een middel om te connecteren met het politie-videonetwerk²⁵;

²⁵ In het functioneel videomodel wordt melding gemaakt van de zogenaamde 4G "Soliton ZAO" videocodec (die in steun kan verkregen worden).

- van de camera's van de dienst DGA/DAS (bijvoorbeeld van de sproeiwagen);
 - van de camera's van diensten extern aan de politie, onder art. 25/2 §2 WPA;
- 3) de CIC's verspreiden op hun beurt de beelden naar de belanghebbende politie-entiteiten:
- van nationaal belang;
 - van eendere welke belanghebbende politie-entiteit die vrijwillig hun beelden met hen deelt;
 - van provinciale derde partijen;
- 4) het video-aanbod wordt vastgelegd in "GPI Videostandaarden" of SVS.

4.5 Rol van CAD in de werkprocessen

38. Bevraagd naar de rol van de CAD in de werkprocessen (stuk 23) stelt het gezamenlijk antwoord van beide politie-entiteiten (stuk 25) (letterlijke weergave):

"Er worden geen beelden in de CAD geïmporteerd.

Enkel wordt er melding gemaakt in de gebeurtenisfiche van de tussenkomst van RTI (nazicht camera's, opzoeken M³. In de CAD is er een layer beschikbaar met de locaties van de camera's. Aan de hand van de pointer van de gebeurtenis, kunnen we opmaken welke camera's er in de buurt aanwezig zijn en dienen te worden gemonitord. De bewaartermijn van tien jaar is een algemeen gegeven binnen de exploitatie van de CAD-gegevensbank".

Met betrekking tot de genoemde "layer" met de locaties van de camera's in CAD, blijkt uit het plaatsbezoek (stuk 30) dat deze apart dienen aangemaakt te worden en dat er geen uitwisseling is met de cameragegevens in het in art. 25/8 WPA voorziene register voor geolocalisatie CamELIA²⁶

4.6 Rol van ISLP in de werkprocessen

39. Bevraagd naar de rol van ISLP in de werkprocessen (stuk 23) stelt het gezamenlijk antwoord van beide politie-entiteiten het volgende (stuk 25):

Vermelding van het bestaan van beelden, PV's neerleggingen.

Er is ook een mogelijkheid om de beelden als bijlage te voegen aan PV's in ISLP.

4.7 Profiel- en toegangsbeheer

40. Uit de analyse blijkt dat het hele proces gematerialiseerd wordt via de koppeling van diverse systemen. Dezelfde analyse van de aangeleverde stukken levert evenwel geen duidelijk en exhaustief beeld op van het profiel- en toegangsbeheer. Hieromtrent bevraagd (stuk 23) stelt het gezamenlijk antwoord van beide politie-entiteiten het volgende (stuk 25) (letterlijke weergave):

"Iedere eerste dag van de maand kijkt men de toegangen na. Bij de uitdiensttreding van een personeelslid neemt men de toegangsrechten af. Aan nieuwe personeelsleden geeft men nieuwe toegangsrechten.

Bij CSD Oost-Vlaanderen gebeuren de toegangen via badges. Wanneer iemand de dienst verlaat worden die toegangsrechten ontnomen.

Nieuwe personeelsleden krijgen een uitzetting door CP Lik waarbij ook RTI wordt uitgelegd.

²⁶In Camelia kunnen de locaties van de politionele camera's en de locaties van camera's van burgers die ter kennis worden gebracht aan de politiediensten geraadpleegd worden. Om de politionele camera's up-to-date te kunnen raadplegen in Camelia, bestaat de mogelijkheid om camera's te creëren, te wijzigen of te verwijderen. De belangrijkste meerwaarde van Camelia is dat de beschikbare camera's van politie en burgers op één unieke plaats raadpleegbaar zijn.

Ieder RTI-lid beschikt over een individuele login en de logins zijn controleerbaar aangezien men die bij DRI kan opvragen".

41. Uit het plaatsbezoek bij de PZ Ninove (stuk 29) blijkt dat het toegangsbeleid tot de VMS gekoppeld is aan graad en functie. Ook blijkt het lokaal waarin de VMS staat niet 24/7 bemand is. Dit heeft onder andere te maken met het aantal interventieploegen dat beperkt is tot 2. De intentie is om het aantal interventieploegen uit te breiden tot 3 (met het oog op het bewaken van een eigen cellencomplex) waardoor de bezettingsgraad van de VMS en dus het cameragebruik zou toenemen.

4.8 Bewaartermijnen in de verschillende systemen

42. Uit de analyse van het COC blijkt dat de gehanteerde bewaartermijnen door elkaar lopen en onduidelijk zijn: 30 dagen versus retrobevraging van 3 uur op VMS versus 48 uur *security desk cam report* versus 24 uur voor het achterliggende script. Hieromtrent bevraagd (stuk 23) stellen beide politie-entiteiten in het gezamenlijk antwoord het volgende (letterlijke weergave):

"Camerabeelden: 30 dagen archivering op VMS, 3 uur rechtstreekse toegang op VMS door RTI.

Voor de communicatie tussen PZ Ninove en RTI maakt men gebruik van een Teamskanaal. Na 24 uren en 59 minuten is er sprake van automatische ventilatie²⁷".

Tijdens het plaatsbezoek in de CSD OVL d.d. 30-04-2024 (stuk 30) wordt opgemerkt dat de bewaartermijn verkeerdelijk werd doorgegeven als zijnde 24 uren. Dit moet 23 uren zijn. Het tonen van de componenten van de werking in de verschillende systemen (stukken 29 en 30) maakt de verschillen in toegepaste bewaartermijnen duidelijk.

Uit het plaatsbezoek aan de PZ Ninove d.d. 30-04-2024 (stuk 29) blijkt dat de toegang tot de VMS van de PZ Ninove ten behoeve van SICAD OVL RTI werd uitgebreid tot 12 uren i.p.v. 3 uren.

Zowel uit de *DPIA* (stuk 7) als uit de plaatsebezoeken (stukken 29 en 30) blijkt dat er, behoudens de verwerkingen van de camerabeelden op het Teamskanaal, geen sprake is van externe (*cloud*) opslag van de beelden²⁸.

4.9 Logbestanden voor de verwerkingen in zijn geheel

43. Gegeven het feit dat de beoogde verwerkingen zich materialiseren in verschillende systemen en componenten is een kennis van de werking van de logbestanden onontbeerlijk teneinde een verwerking *end-to-end* te kunnen traceren en documenteren. Evenwel blijven de *DPIA* (stukken 7 en 8) daar zeer vaag over, of spreken deze stukken over de logbestanden in zeer algemene termen, dan wel definities. Tijdens de plaatsbezoeken (stukken 29 en 30) worden volgende aspecten toegelicht:

- de VMS van de PZ Ninove beschikt over een eigen beheer van de reden raadpleging (stuk 29);
- de logbestanden voor het documenteren van de toegangen tot de camera's, enerzijds, en tot de VMS van zowel de PZ Ninove als de CSD OVL, anderzijds, worden beheerd door DGR/DRI;
- aan beide politie-entiteiten werd door het COC de suggestie gemaakt om, daar waar de applicaties geen eigen mogelijkheid hebben om een reden van raadpleging in te geven, te overwegen of een registratie van de reden van raadpleging middels de centrale logging in Portal een optie is.

²⁷ Automatische ventilatie in de zin van het vermelde citaat dient begrepen te worden als zijnde automatische wissing.

²⁸ De leverancier van de VMS biedt zulks aan.

4.10 Privacy-protocol

44. Middels stuk 6 wordt tevens een privacy-protocol (stuk 9) overgemaakt dat gedateerd is op 07-07-2022, dus nà de start van de verwerking en nà de opening van het toezichtonderzoek door het COC, en getekend werd door de DirCo OVL op 11-07-2022. Een handtekening van de (korpchef van de) PZ Ninove ontbreekt. Hieromtrent bevroegd (stuk 23²⁹,) stelt het gezamenlijk antwoord van de beide politie-entiteiten het volgende (stuk 25) (letterlijke weergave):

"Protocol 2022 i.p.v. 2020.

Start Teamskanaal 22/10/2020

Start verwerking beelden (via een test) 07/02/2022".

Opnieuw stelt DOSE vast dat dit stuk herhaaldelijk refereert aan de AVG, wat in het raam van de operationele, politionele verwerkingen niet van toepassing is. Rechtstreekse verwijzingen naar het van toepassing zijnde rechtskader inzonderheid de titel 2 WVG en de artikelen 25/1 tem 25/8 WPA³⁰ ontbreken.

4.11 Didactisch gebruik van de camerabeelden

45. Bevroegd (stuk 23) naar een eventueel didactisch gebruik ingevolge het punt 6.3 van stuk 7 geïnsinueerde "6.3 *Didactische en pedagogische doeleinden zijn toegestaan in het kader van de opleiding van de leden van de politiediensten na anonimisering*" luidt het gezamenlijk antwoord van beide politie-entiteiten als volgt (letterlijke weergave):

"Voor beide partijen, politiezone Ninove & CSD Oost-Vlaanderen, niet van toepassing."

5 JURIDISCH – TECHNISCH – FUNCTIONEEL KADER

5.1 Inleiding

46. In wat hieronder volgt, worden de vaststellingen van de onderzoeksbevindingen afgetoetst aan het vigerende juridische, technische en functionele kader. Wanneer dit juridisch kader reeds eerder werd toegelicht in andere rapporten van het COC wordt daaraan gerefereerd.

Eens te meer blijkt de noodzaak tot het samenlezen van de bepalingen van de Ministeriële richtlijnen informatieveiligheid, koppelingen en toegangen, naast de wettelijke bepalingen in de WVG en de WPA en deze toe te passen in de *DPIA* en in de procesmodellen.

5.2 Relatie tussen de actoren op vlak van het gegevensbeschermingsrecht

5.2.1 Verwijzing naar een bestaand rapport

Het COC verwijst hiervoor naar het rapport DIO23004³¹, inzonderheid het punt 5.6; randnummers 40 tem 45.

5.2.2 Verwerker of leverancier

²⁹ Het stuk 23 bevat onder punt 1.6. in deze foutief de datum van 07-07-2020 hetgeen uiteraard gelezen dient te worden als 07-07-2022.

³⁰ Op 07-07-2022 was er nog geen sprake van het artikel 25/9 WPA, in voege getreden bij Wet van 19-10-2023.

³¹ Toezichtrapport DIO23004 van 25 april 2024 van het Controleorgaan op de politionele informatie in het raam van zijn controle en toezichtsbevoegdheden n.a.v. de inzet van een mobiele camera middels een drone in het raam van interzonale steunverlening, niet gepubliceerd, te vinden op de *Sharepoint* GPI, Pagina REGPOL, <https://bpolb.sharepoint.com/sites/regpol/Publications%20COC%20%20Publicaties%20COC/Forms/AllItems.aspx>

47. Bijkomend wenst het COC evenwel aandacht te besteden aan het onderscheid tussen een verwerker dan wel een leverancier. Om te bepalen of de leverancier van een product of een dienst ook een verwerker is, is het van cruciaal belang om bij het afdraaien van de voorwaarden na te gaan, of deze externe entiteit *überhaupt* persoonsgegevens verwerkt. Wanneer de dienstverlening in opdracht van de verwerkingsverantwoordelijke zich louter beperkt tot het leveren van een softwarepakket, applicatie, hardware zoals servers of camera's of een combinatie al dan niet met inbegrip van onderhoud en/of het louter leveren van IT ondersteuning zonder daarbij onvermijdelijk persoonsgegevens te verwerken is deze leverancier geen verwerker³². De nadruk van de relatie ligt immers elders. Ook wanneer deze leverancier in dezelfde voormelde omstandigheden hetzij vanop afstand hetzij *on premise* tijdelijk toegang krijgt tot het systeem om bijvoorbeeld onderhoudswerken uit te voeren, opleidingen te geven dan wel incidenten op te lossen is de leverancier geen verwerker. In deze gevallen is het afsluiten van een verwerkingsovereenkomst dan ook niet nodig. **Wel is het ten sterkste aanbevolen, om een geheimhoudingsclausule of NDA³³ af te sluiten.** Immers, het valt niet uit te sluiten dat bij het uitvoeren van de afgesproken taken, de leverancier accidenteel doch niet structureel (intentioneel) te maken krijgt met politionele gegevens. Ook moet gewaarschuwd worden voor situaties waarbij de verwerkingsverantwoordelijke te veel afhankelijk is van de leverancier, en niet zomaar kan overschakelen naar een andere zonder het maken van substantiële kosten³⁴.

5.3 Koppelen (delen) van politiegegevens

5.3.1 De Ministeriële richtlijn koppelingen

48. De Ministeriële richtlijn koppelingen³⁵ omschrijft de koppeling als een vorm van gegevensverwerking in de zin van artikel 26. 2° WVG, die toelaat om gegevens te delen tussen personen die er in het kader van hun wettelijke opdrachten nood aan hebben. De koppeling maakt het tevens mogelijk een meerwaarde toe te voegen aan de oorspronkelijk verwerkte gegevens door ze te correleren en te verrijken. Het delen en verrijken van politiegegevens (informatie en persoonsgegevens) is een basisgegeven voor een informatie-gestuurde politiezorg, en het koppelen van gegevensbanken zou de regel moeten zijn van het beheer van operationele politionele informatie, gebaseerd op een adequaat en gedifferentieerd profiel- en toegangsbeheer (zie infra punt 4.4.).

Concreet kan deze richtlijn gematerialiseerd worden via volgende acties:

- 1) via één zoekopdracht gegevens raadplegen die oorspronkelijk in verschillende gegevensbanken worden verwerkt en die dus verspreid zitten;
- 2) gegevens die oorspronkelijk in verschillende gegevensbanken zijn verwerkt, met elkaar correleren, of verbanden leggen tussen deze gegevens, aan de hand van analysetools of analyse-applicaties of, in voorkomend geval, aan de hand van lijsten of uittreksels, doch rekening houdende met noodzaak en proportionaliteit door het nemen van gepaste technische en organisatorische maatregelen;
- 3) gegevens verrijken door interne referentiebronnen naast externe referentiebronnen te leggen.

De volgende voorwaarden en modaliteiten zijn van toepassing:

- 1) relevantie van de gegevens naast de *need-to-know* van het profiel, alsmede diens maturiteitsniveau, opleiding en ervaring (zie ook infra punt 5.4);
- 2) duidelijkheid omtrent de validatiestatus van de gegevens;
- 3) de categorie van betrokkenen waartoe de in de operationele politionele gegevensbanken geregistreerde persoon behoort moet ondubbelzinnig kunnen worden geïdentificeerd (dader, slachtoffer, getuige, ...);

³² Zie European Data Protection Board (EDPB), *Richt snoeren 07/2020 over de begrippen "verwerkingsverantwoordelijke" en "verwerker" in de AVG*, vastgesteld op 7 juli 2021, p. 31-32 *in fine*.

³³ Non Disclosure Agreement: overeenkomst waarbij de betrokken partijen met elkaar afspreken bepaalde informatie geheim te houden en dus niet met anderen te zullen delen.

³⁴ Vendor lock-in en path-dependency.

³⁵ Gemeenschappelijke bindende richtlijn van 4 augustus 2021 van de Ministers van Justitie en van Binnenlandse Zaken aangaande de nadere regels betreffende de koppeling van de gegevensbanken bedoeld in artikel 44/2 WPA onderling of met andere gegevensbanken waartoe de politiediensten toegang hebben door of krachtens de wet of internationale verdragen die België binden.

- 4) behoudens overmatigheid, de voorafgaande of gelijktijdige raadpleging van de ANG, die ook correct moet gevoed worden;
- 5) naleven van de regels van toegang en bewaartermijnen;
- 6) identificatie van origine van de gegevens (transparantie);
- 7) registratie van de verwerking in RegPol;
- 8) actualisering van de gegevens conform art 44/5 § 6 WPA (en bij uitbreiding in toepassing van art 646 Sv);
- 9) aanwezigheid van logbestanden met inbegrip van de reden raadpleging;
- 10) analysetools en applicaties moeten auditeerbaar zijn;
- 11) ontwikkelen van een beleid inzake systematische en proactieve controles op het gebruik en/of de raadpleging van politionele gegevensbanken.

De wijze waarop deze acties, voorwaarden en modaliteiten toegepast worden moet derhalve blijken uit de *DPIA*.

5.3.2 Koppelingen binnen het proces van de politionele cameraverwerkingen

49. Het COC wenst te verwijzen naar eerder geformuleerde aanbevelingen in het kader van een efficiënt en geïntegreerd beheer van het politioneel cameragebruik³⁶.

5.3.3 De rol van *MS Teams* bij de koppelingen binnen het proces van de politionele cameraverwerkingen

50. *MS Teams* speelt zowel in de verwerking van de CSD OVL en de PZ Ninove, als in het functioneel videomodel (stuk 17), een rol. Bij de CSD OVL en de PZ Ninove geldt *MS Teams* als kanaal om beelden en foto's snel ter beschikking te stellen van ploegen op het terrein. Uit het functioneel videomodel (stuk 17), alsmede het antwoord van DGA/DAFA (stukken 20 en 22), blijkt dat de rol van *MS Teams* in hoofdzaak beperkt is tot het kunnen raadplegen van de beelden in *real time* middels schermdeling en dat ingevolge technische pannes dan wel het ontbreken van een alternatief. Uit de antwoorden van DGA/DAS (stuk 21) blijkt een gelijkaardige behoefte door te refereren aan een meerwaarde bij testen tijdens "*live situaties*". Bovendien blijkt de interesse voor *MS Teams* ook aanwezig bij andere politie-entiteiten die een behoefte hebben om grote bestanden met beeldverwerkingen aan een eindgebruiker te kunnen bezorgen³⁷.

Op geen enkel ogenblik lijkt *MS Teams* een rol te spelen als captatiemiddel (een individuele politieambtenaar gebruikt de camera van zijn smartphone om beelden te verzamelen en door te sturen naar een *VMS*) noch als ontvangstmiddel – behoudens via schermdeling – van camerabeelden. Met andere woorden, *MS Teams* lijkt ook op dit vlak geen *conditio sine qua non* te zijn om een functioneel videmodel uit te bouwen.

51. Het functioneel videomodel (stuk 17) refereert evenwel aan alternatieven die aan de gedetecteerde behoeften voor het volgen van gebeurtenissen in *real time* zouden kunnen voldoen, alsmede aan de behoefte tot het raadplegen van beelden achteraf, zonder dan nog te spreken over een eventuele integratie met de mogelijkheden van het FOCUS platform. De terechte vraag is dan ook of, na toepassing van dit functioneel videomodel, er *überhaupt* nog een noodzaak is tot het gebruiken van *MS Teams* binnen de politionele verwerkingen, inzonderheid op het vlak van de koppelingen. Hierbij moet worden opgemerkt dat uit een rapport van 2022³⁸ (stuk 31) over het gebruik van de toepassing *MS-Teams* van het Nederlandse Ministerie van Justitie en Veiligheid zeven lage risico's en één hoog risico blijken. Het hoge risico heeft met name te maken met de mogelijke toegang van opsporings- en inlichtingendiensten uit de VS tot zeer gevoelige en bijzondere persoonsgegevens waardoor wordt aangeraden om geen gevoelige bestanden uit te wisselen via *MS Teams* (of bij uitbreiding ook *Sharepoint/ OneDrive*), tenzij ze vooraf geëncrypteerd werden met sleutels in eigen beheer. Tevens wordt aangeraden om geen gevoelige informatie te delen via online *meetings/calls* (*Teams/ Streams*). Zonder afbreuk te doen aan het geheel van geïdentificeerde risico's aan het gebruik van inzonderheid *MS Teams* heeft *Microsoft* onder meer nog geen *end-to-end-encryption* (E2EE) voorzien voor *MS Teams* meetings. Met andere woorden, de 'opnames'³⁹ van de meetings (groepsvergaderingen en chats) zijn in *clear* tekst beschikbaar op de *Microsoft* servers.

³⁶ CON20004, DIO20009/1, DIO23004.

³⁷ DIO23004 (niet openbaar gemaakt).

³⁸ *DPIA on Microsoft Teams, OneDrive Sharepoint and Azure AD (June 2021), Data protection impact assessment on the processing of Diagnostic Data*, version 1.1, Ministerie van Justitie en Veiligheid, 16-02-2022.

³⁹ Met opnames wordt bedoeld: beeld en geluid, gebruikte bestanden en chats, metadata,

Verder onderzoek van dezelfde bron⁴⁰ (stuk 32) wijst uit, dat *Microsoft* maatregelen heeft getroffen om zes hoge risico's te verhelpen, maar dat organisaties deze *cloud*diensten niet mogen gebruiken voor de uitwisseling of opslag van gevoelige en bijzondere persoonsgegevens. Dat mag alleen als ze de inhoud kunnen versleutelen met eigen sleutels. Dit komt door het hoge risico van mogelijke toegang tot die gegevens vanuit de Verenigde Staten. Dit risico blijft bestaan ook als *Microsoft* (contractueel) vrijwel alle persoonsgegevens van haar Europese zakelijke klanten (beweerdelijk) exclusief in Europese datacentra⁴¹ verwerkt.

Gekoppeld aan de onduidelijkheden omtrent gebruikersbeheer en logbestanden en de verregaande mogelijkheden om ook externen aan de organisatie op eenvoudige wijze toegang te verlenen en bestanden te delen maakt dit dat het gebruik van *MS Teams* niet als zonder risico kan aanzien worden. Een beslissing van de *EDPS*⁴² van 8 maart 2024 tot het nemen van een corrigerende maatregel t.a.v. de Europese Commissie n.a.v. het schenden van verschillende regels inzake gegevensbescherming bij het gebruik van *Microsoft* toepassingen wijst in dezelfde richting. Hoewel het gebruik van *Microsoft* oplossingen binnen de GPI hoe langer hoe meer een standaard praktijk wordt zal permanent dienen toegezien moeten worden op de complementariteit met het vigerend gegevensbeschermingsrecht. Daarmee is dan zelfs nog niets gezegd over de actuele geopolitieke context en de ook in dat kader inherente risico's bij het (exclusief) gebruik van (Amerikaanse) zgn. 'big tech' of GAFAM⁴³ applicaties.

5.3.4 Hybride werken⁴⁴

51. De geïntegreerde politie ontsnapt niet aan de maatschappelijke evolutie van het hybride werken, met name een vorm van werken waarbij deels vanop afstand, bijvoorbeeld middels thuiswerk, dan wel op de fysieke werkplek, met name in een politiekantoor of op het terrein, wordt gewerkt. Uiteraard moeten de medewerkers daarvoor apparaten gebruiken – radiomiddelen, laptops, smartphones of tablets die hetzij eigendom zijn van het personeelslid dan wel ter beschikking worden gesteld door de organisatie, alsmede toegangskanalen zoals vaste of mobiele netwerken op locatie of op de werkplek, hotspots, VPN verbindingen, enz. ... Wanneer een organisatie ervoor kiest om *BYOD* toe te passen, is er nood aan een degelijk beleid hieromtrent, waaronder de beveiliging, alsmede de maatregelen die de medewerker moet nemen. Tevens moet duidelijk zijn voor de medewerkers wat zij kunnen, maar vooral wat zij niet mogen doen (en kunnen) met hun apparaten. In geen geval mag een dergelijk beleid unilateraal worden opgelegd, met bijvoorbeeld verspreiding van persoonlijke gegevens van de medewerkers (privénummers, privé emailadressen, enz. ...). De problematiek van *BYOD* wordt niet verder uitgewerkt in dit rapport.

5.4 Toegang tot politiegegevens

5.4.1 De Ministeriële richtlijn toegangen

⁴⁰ <https://www.privacycompany.eu/blogpost-nl/nieuwe-dpia-voor-de-rijksoverheid-en-universiteiten-op-microsoft-teams-onedrive-en-sharepoint-online>

⁴¹ Zoals vermeld in punt 13 van de minimale beveiligingsmaatregelen van de Ministeriële richtlijn informatieveiligheid van 13.07.2021.

⁴² European Data Protection Supervisor, de onafhankelijke toezichthoudende autoriteit die erop toeziet dat de Europese instellingen en organen het recht op privacy en gegevensbescherming in acht nemen wanneer zij persoonsgegevens verwerken en nieuwe beleidslijnen ontwikkelen.

⁴³ Google, Apple, Facebook (thans Meta), Amazon en Microsoft.

⁴⁴ Die kunnen worden uitgebreid met *BYOD*, *CYOD* en *COPE*:

- *Bring Your Own Device*: de medewerker gebruikt op vrijwillige basis zijn eigen apparaten. De beveiliging is niet uniform, hangt af van de gebruiker en is daardoor vaak minder goed verzekerd; het apparaat wordt ook privé gebruikt en het apparaat management is complex(er) voor de organisatie.

- *CYOD: Choose Your Own Device*: de medewerker kan kiezen uit een (beperkt) aanbod van apparaten die eigendom zijn van de organisatie. De beveiliging is de verantwoordelijkheid van de organisatie en is vaak hoger. Het apparaat mag NIET privé worden gebruikt en het apparaat management is minder complex voor de organisatie.

- *COPE: Company issued Personally enabled*: de organisatie voorziet apparaten die de medewerkers ook privé kan gebruiken. De beveiliging is de verantwoordelijkheid van de organisatie en is vaak hoger. Het apparaat mag privé worden gebruikt en het apparaat management is minder complex voor de organisatie.

52. De Ministeriële richtlijn toegangen⁴⁵ benadrukt het *need-to-know* beginsel als uitgangspunt voor toegangen tot de ANG, de basisgegevensbanken, de technische gegevensbanken en de bijzondere gegevensbanken. De leden van de politiediensten worden voorafgaandelijk elke toegang tot de gegevensbanken en de gegevens die ze bevatten geïdentificeerd en geauthentiseerd en elke toegang wordt gelogd. De korpschefs voor de lokale politie en de commissaris-generaal en de directeurs (-generaal) voor de federale politie beslissen voor de leden van hun personeel welke toegang noodzakelijk is om de hun toevertrouwde taken uit te voeren en bepalen hieromtrent een toegangsbeleid, dat de voorgeschreven regels weerspiegelt en in overeenstemming is met de lokale situatie waarvoor zij verantwoordelijk zijn. Om te bepalen of een toegang tot een gegevensbank noodzakelijk is, steunen de genoemde gemandateerden zich inzonderheid op:

- 1) de doeleinden bepaald in de WPA voor de gegevensbank in kwestie;
- 2) de categorieën van personen bedoeld in artikel 44/5 van de WPA;
- 3) het evaluatieniveau van de gegevens;
- 4) het validatieniveau van de gegevens;
- 5) het vereiste profiel om er toegang toe te krijgen;
- 6) het toegangsrechten en wat zij toelaten.

Bijzondere aandacht is noodzakelijk voor een toegang tot persoonsgegevens betreffende de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging, het lidmaatschap van een vakvereniging, de gezondheid, seksueel gedrag of seksuele gerichtheid en in het geval van verwerking van genetische of biometrische gegevens.

Tevens dient er een onderscheid gemaakt te worden tussen het permanente dan wel tijdelijke karakter van de toegang.

Ook een passend kennisniveau wordt benadrukt.

Bij voorkeur worden de toegangen beheerd middels een op rollen gebaseerd rechtensysteem als centraal register voor profielen en toegangen, met uitzonderingen voor de bijzondere gegevensbanken en de lokale technische gegevensbanken. Toegangsbeheer is een dynamisch proces met regelmatige *updates*, zodat alleen de noodzakelijke toegangen actief zijn. Minstens eenmaal per jaar moeten hierop controles plaatsvinden.

Identificatie, authenticatie en logging met inbegrip van de verplichting tot multifactor authenticatie (MFA) zijn essentieel binnen het toegangsbeheer.

5.4.2 Toegepast *in casu*: toegangen binnen een complex systeem van gekoppelde cameraverwerkingen

53. Uitgaande van de vigerende regelgeving en de aanname dat een *VMS* dient aanzien te worden als een bijzondere gegevensbank, lijkt het toegangsbeheer voor de diversiteit aan systemen zoals *in casu* maar zeker in het functioneel videomodel (stuk 17) geen gemakkelijke opgave. Hoewel de Ministeriële richtlijn koppelingen de koppeling van bijzondere gegevensbanken toelaat is een beheer van de toegangen, indien dit telkens vanuit een lokaal register dient geregeld te worden, tot zelfs beheerd wordt door een enkele leverancier, geen sinecure, zeker niet in een concept zoals het functioneel videomodel (stuk 17) omschrijft, laat staan een *end-to-end* reconstructie van een verwerking middels de logbestanden. Een centraal beheer van dergelijke toegangen alsmede een centrale logging van de verwerkingen *end-to-end* dringt zich op. Het COC verwijst hierbij onder meer naar de toepassing van de zogenaamde AAA (authenticatie, autorisatie en accounting) in het raam van:

- de rol van een diversiteit aan beheersystemen zoals LDAP, PolBacc, ACC, LORI, Active Directory en hun onderlinge verhouding en dit in relatie tot een centraal register van profielen en toegangen zoals vermeld in punt III van de genoemde Ministeriële richtlijn d.d. 13-07-2021;
- de rol van de bron voor het personeelsbeheer van de geïntegreerde politie en de wijze waarop dit in de individuele diensten van de federale politie of zones van de lokale polities wordt gematerialiseerd, alsmede de afgeleide processen zoals het telefoonregister CRC en de emailadressen police.belgium.eu;
- het beheer van toegangen binnen een applicatie zelf;

⁴⁵Gemeenschappelijke bindende richtlijn van de Ministers van Justitie en van Binnenlandse Zaken van 13 juli 2021 met betrekking tot de toegangsregels van de leden van de politiediensten tot de algemene nationale gegevensbank en de basis-, bijzondere en technische gegevensbank.

- het onderscheid tussen medewerkers intern (Ops/CaLog) en medewerkers extern aan de GPI evenals alle externe partijen die gebruik maken van informatie van de politie⁴⁶.

54. In de huidige politieomgeving lijkt het vooralsnog niet te vermijden dat gegevens verder verspreid worden via externe dragers. De (functioneel) verwerkingsverantwoordelijken moeten dan ook de nodige technische en organisatorische maatregelen nemen om met deze realiteit om te gaan. In dergelijke context is het risico op ongecontroleerd verspreiden van gegevens groot en de controle moeilijk. Dit risico zou gemitigeerd kunnen worden door:

- organisatorisch vast te leggen in welke (limitatieve) omstandigheden er kan gebruik gemaakt van externe dragers;
- technisch gebruik te maken van versleuteling van de gegevens op de drager.

5.5 De risico- en impactanalyses

5.5.1 Soorten impact- en risico analyses

55. Het COC verwijst hiervoor naar het rapport DIO23004 voornoemd⁴⁷, inzonderheid het punt 5.3, randnummers 34-36.

5.5.2 Een referentie *DPIA* voor gelijkaardige verwerkingen

56. Het COC verwijst hiervoor naar het rapport DIO23004 voornoemd, inzonderheid het punt 5.3, randnummer 37.

5.5.3 Toegepast *in casu*: naar referentie *DPIA's* voor politionele cameraverwerkingen

57. De initiële onduidelijkheden uit de eerste analyse van de stukken 7 t.e.m. 11 in samen lezing met bepaalde van de verkregen antwoorden in stuk 25 tonen aan dat het opmaken van een *DPIA* een complexe oefening is, die een stevige juridische, technische en functionele kennis vereist alsmede een goede coördinatie tussen de daarbij betrokken actoren. Gegeven het functioneel videomodel van de GPI (stuk 17), alsmede de complexiteit voor het maken van dergelijke analyses, lijkt het ook in deze beter om één *DPIA* te maken van dit functioneel model, bijvoorbeeld op nationaal niveau, waarna deelprojecten om tot dit model te evolueren, zoals *in casu*, kunnen afgetoetst worden, al dan niet in combinatie met een daarmee corresponderende, doch gereduceerde, referentie *DPIA*.

5.6 Registers

58. Door de wet van 19 oktober 2023 werd ook artikel 25/8 WPA gewijzigd en is er geen sprake meer van een lokaal register van alle gebruiken van camera's. Thans is voorzien dat alle cameraverwerkingen moeten worden bijgehouden in het unieke register van verwerkingsactiviteiten van de politiediensten bedoeld in artikel 145 WGP (RegPoL), waardoor tegelijk het gebruik van camerabewaking kan afgetoetst worden aan het register van de verwerkingsactiviteiten. Ook het register geolocalisatie moet worden bijgehouden. Het zou naar het oordeel van het COC overigens een operationele meerwaarde zijn als er een synchronisatie zou plaatsvinden tussen dit unieke register geolocalisatie CamELIA enerzijds, en het CAD systeem anderzijds, of, bij uitbreiding, tussen het unieke register geolocalisatie CamELIA en elke andere politionele toepassing die werkt met camera locaties.

⁴⁶ Bijvoorbeeld in toepassing van artikel 25/5 §2 WPA bij het beheer van grootschalige evenementen dan wel onverwachte incidenten die in het raam van de crisis- en noodplanning multidisciplinair worden aangepakt.

⁴⁷ Toezichtrapport DIO23004 van 25 april 2024 van het Controleorgaan op de politionele informatie in het raam van zijn controle en toezichtsbevoegdheden n.a.v. de inzet van een mobiele camera middels een drone in het raam van interzonale steunverlening, niet gepubliceerd, te vinden op de *Sharepoint* GPI, Pagina REGPOL, <https://bpolb.sharepoint.com/sites/regpol/Publications%20COC%20%20Publicaties%20COC/Forms/AllItems.aspx>

5.7 Testen van politionele toepassingen

59. In subsidiaire orde blijkt uit een van de antwoorden uit de diverse vraagstellingen (stuk 21) opnieuw de behoefte om de correcte werking van politionele toepassingen te kunnen testen. Ten overvloede moet het COC hier verwijzen naar eerdere conclusies⁴⁸ ⁴⁹ dat de verwerking van politionele informatie en persoonsgegevens (politiegegevens) met het oog op het (uit)testen, in een experimentele fase, zou moeten geregeld worden teneinde een helder en sluitend juridisch kader te krijgen.

5.8 Didactisch gebruik van camerabeelden

60. Het didactisch gebruik van beelden zoals voorzien in art 25/7 § 2 WPA is een andersluidende finaliteit, daar deze uitdrukkelijk beperkt is tot didactische en pedagogische doeleinden in het kader van de opleiding van de leden van het operationeel of logistiek kader van de politiediensten en dit bovendien na anonimisering.

6 TOEPASSING VAN DE VASTSTELLINGEN IN DE HUIDIGE CASUS EN HET FUNCTIONEEL VIDEOMODEL IN HET LICHT VAN DE VISIE VAN HET COC – SUGGESTIES VOOR TOEKOMSTIGE OPTIMALISATIE BINNEN DE GPI.

6.1 Inleiding

61. Het afoetsen van het functioneel, technisch en regelgevend kader aan de concrete casus van de cameraverwerkingen door de CSD OVL ten behoeve van de PZ Ninove in het licht van een geïntegreerde visie op het politioneel cameragebruik, zoals eerder al bepleit door het COC - en dit naast het functioneel videomodel zoals in evolutie bij de GPI - resulteert in een aantal suggesties voor verdere toekomstige optimalisatie binnen de GPI. Deze suggesties zijn evident niet-dwingend en moeten dan ook aanzien worden als een uitnodiging voor verder onderzoek en reflectie.

Het COC werd daarbij geconfronteerd met een initiatief uitgaande van een federale steunentiteit en een lokale politie entiteit om een goede operationele steun te kunnen verlenen aan bepaalde operaties van de lokale politie door gebruik te maken van bestaande en beschikbare middelen in een context van beperkte investeringsbudgetten. Aldus ontstaat een cultuur van (supra)-lokale en creatieve *ad-hoc* opstellingen teneinde tegemoet te komen aan een gerechtvaardigde operationele behoefte. Nochtans bestaat er een verdedigbaar conceptueel model dat evenwel omwille van budgettaire beperkingen niet ten volle kan worden uitgerold. Dit leidt evident tot een aantal niet onbelangrijke vraagstukken, zoals de rol van verwerkingsverantwoordelijken, verwerkers en leveranciers, het behandelen van een complexe *DPIA*, vraagstukken omtrent koppelingen van systemen en vraagstukken omtrent toegangsbeheer (met inbegrip van autorisatie, authenticatie en audit). De aanpak van deze vraagstukken vereist een juridische, technische en functionele kennis die het niveau van de rechtstreeks betrokken actoren geregeld overstijgt en een gecoördineerde, eerder nationale benadering vergt. De complexiteit wordt zeker niet vereenvoudigd door de wettelijke verplichting om te moeten vasthouden aan het koppelen van politionele verwerkingen van gegevensbanken in de WPA.

Deze suggesties overstijgen bijgevolg de loutere casuïstische vaststellingen van dit rapport, alsmede de individuele verantwoordelijkheid van de betrokken korpschef en directeur en noodzaken eerder een GPI brede benadering van de toepassing van het politionele gegevensbeschermingsrecht in relatie tot het toegangsbeheer en het koppelen van systemen tussen de verschillende lokale en federale politiezones en -diensten. De hierna uitgebrachte suggesties zijn dan ook gericht aan de beleidsverantwoordelijken op elk niveau, met inbegrip van de voogdijministers.

⁴⁸ Aanbeveling 2 uit het toezichtrapport DIO21006 van 04 februari 2022 van het Controleorgaan op de politionele informatie met betrekking tot het gebruik van Clearview ai door de geïntegreerde politie;

⁴⁹ Aanbeveling 3 uit het toezichtrapport DIO23001 van 02 mei 2023 van het Controleorgaan op de politionele informatie in het raam van zijn controle- en toezichtsbevoegdheden n.a.v. de verwerkingen in de ANG van inbreuken begaan door leden van de geïntegreerde politie.

6.2 Normering van politionele verwerkingen, niet noodzakelijk van politionele gegevensbanken

62. Noch de Richtlijn *LED*, noch de WVG vereisen dat politiegegevensbanken opgericht worden. De nadruk ligt in deze teksten immers op wettelijkheid, noodzaak en proportionaliteit van 'verwerkingen', finaliteiten, (categorieën van) persoonsgegevens en niet *ab initio* op de drager of het verwerkingsstelsel als dusdanig⁵⁰. De oprichting van een gegevensbank is eerder een pragmatische keuze. Toch bepaalt de WPA restrictief welke gegevensbanken opgericht worden en welke types van persoonsgegevens in deze gegevensbanken verwerkt worden. Opdat de persoonsgegevens rechtmatig bijgehouden (en gebruikt) worden, moeten de persoonsgegevens dus aan een bepaalde politionele gegevensbank toegewezen kunnen worden. In dat opzicht houdt dat in zekere zin een beperking in op de politionele verwerkingen, hetgeen deze casus ten overvloede illustreert. Het vasthouden aan gegevensbanken lijkt enkel nuttig wanneer deze gegevensbank een op zich staande finaliteit heeft, zoals bijvoorbeeld het Rijksregister of de Kruispuntbank van de voertuigen. Een opportuniteit biedt zich kennelijk ook aan, nu het Regeerakkoord voor de periode 2025-2029 (hoofdstuk "Veiligheid", onderdeel "Opsporing en Informatiedeling") specifiek melding maakt van nieuwe wetgeving: "In navolging van de EU richtlijn 2016/680 werd in de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens reeds voorzien in de omzetting van deze richtlijn voor de specifieke toepassing zijnde de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op het voorkomen, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen. De beschrijving van de verwerkingen zelf wordt vandaag geregeld in de wet van 5 augustus 1992 op het politieambt en het wetboek van strafvordering. **In een volgende stap wordt er een wettelijk kader gecreëerd door een specifieke Wet op politionele gegevens**, om deze zaken samen te voegen. In deze wet worden de rechten en plichten van zowel de politie als van de burger inzake het verwerken van politiegegevens geregeld. ..."⁵¹

6.3 Keuze voor het bepalen van de juridische relatie tussen (functioneel) verwerkingsverantwoordelijken, verwerker en leverancier

63. De operationele relatie tussen de het SICAD OVL als steunverlener, enerzijds, en de PZ Ninove die wordt ondersteund, anderzijds, lijkt zich niet zonder meer te kunnen worden doorgetrokken op het vlak van verantwoordelijkheden gedefinieerd binnen het gegevensbeschermingsrecht. Enerzijds zijn de wederzijdse opdrachten en bevoegdheden gedefinieerd in de WGP, inzonderheid artikel art 104 *bis* en het KB van 26 juni 2002⁵². Anderzijds gaat het om verwerkingen die, ingevolge de keuze van de wetgever, plaatsvinden in politionele gegevensbanken. Voor de politionele cameraverwerkingen worden in de WPA de volgende verwerkingsverantwoordelijken gedefinieerd:

- art 25/5, dat verwijst naar de artikelen t.e.m. 7 tot en met 7/3 WPA, zijnde de korpschef of de directeur-coördinator;
- art 44/11/3 *sexies*, dat evenwel enkel betrekking heeft op de technische gegevensbanken, die ingevolge artikel 44/2 beperkt zijn tot intelligente camera's of systemen met het oog op automatische nummerplaatherkenning, en die hetzij de korpschef, voor wat betreft de lokale technische gegevensbanken, dan wel de Ministers van Binnenlandse Zaken en Justitie, voor wat betreft de nationale technische gegevensbank aanduidt als verwerkingsverantwoordelijke

Ingevolge de logica van de wetgever om politionele gegevensverwerkingen te laten plaatsvinden in gegevensbanken, en bij ontstentenis van een duidelijke omschrijving van welk type gegevensbank een *VMS* is, lijkt dus enkel art 44/11/3 WPA ingeroepen te kunnen worden als rechtsgrond voor de gegevensbanken waarbinnen cameraverwerkingen plaatsvinden. In die zin lijkt er voor de *VMS* (to *VMS*) communicatie die aldus plaatsvindt een relatie van toepassing te kunnen zijn van "gezamenlijke verwerkingsverantwoordelijke" van een verwerking van persoonsgegevens in een bijzondere gegevensbank in de zin van art 44/11/3 WPA. Deze zienswijze lijkt in alle geval ondersteund te worden door

⁵⁰ Vgl. R. SAELENS, "De Wet op het politieambt na de Aanpassingswet van 22 mei 2019 in het licht van de Richtlijn Politie en Justitie: een beknopte verkenning van de verwerking van persoonsgegevens voor opdrachten van bestuurlijke en gerechtelijke politie", in F. GOOSSENS, K. DE PAUW, F. VERSPEELT (eds.) *De sluier rond anonimiteit opgelicht ... Identiteits-, privacy- en persoonsgegevensafscherming in het strafprocesrecht en politierecht*, die Keure 2022, 316-318.

⁵¹ Federaal Regeerakkoord 2025-2029, p. 133, www.belgium.be/sites/default/files/resources/publication/files/Regeerakkoord-Bart_De_Wever_nl.pdf
⁵² KB van 26 juni 2002 betreffende de organisatie van de gecentraliseerde dispatchingcentra en van het nationaal invalspunt, *BS*, 15 augustus 2002.

een uitspraak van het Europees Hof van Justitie⁵³, waarin het Hof erop wijst dat het zelfs niet nodig is om een wettelijke regeling van vaststelling van bepaling van doel en middelen te hebben tussen twee entiteiten om hen te aanzien als gezamenlijke verwerkingsverantwoordelijken. Daarbij moeten de betrokken korpschefs hun respectieve verantwoordelijkheden voor de nakoming van de verplichtingen op transparante wijze vaststellen door middel van een onderlinge regeling. Evenwel vormt het bestaan van een dergelijke regeling geen voorafgaande voorwaarde om twee of meer entiteiten als "gezamenlijke verwerkingsverantwoordelijken" te (kunnen) kwalificeren, maar een verplichting die de LED/WVG oplegt, en dit van zodra zij als verwerkingsverantwoordelijken zijn gekwalificeerd. Dit moet toelaten de op hen rustende verplichtingen van de WVG en de WPA te verzekeren. De gezamenlijke verantwoordelijkheid veronderstelt niet noodzakelijk een gelijkwaardige verantwoordelijkheid van de betrokken korpschefs voor de gezamenlijke verwerking. Iedere betrokken korpschef kan in verschillende fasen en in verschillende mate bij de verwerking betrokken zijn, zodat het niveau van de verantwoordelijkheid moet worden beoordeeld in het licht van de concrete omstandigheden van de verwerking.

Verder dient er bepaald te worden wat de exacte rol is van bepaalde derde partijen. Gaat het om verwerkers dan wel om leveranciers? Binnen de casus lijken de (functioneel) verwerkingsverantwoordelijken met betrekking tot de onderdelen van het proces en de gebruikte systemen en *tools* daaromtrent een andere visie te hebben dan DRI, ondanks het bestaan van een korpsnota daaromtrent. Ook kan men niet spreken van een leverancier als zijnde verwerker, wanneer er geen sprake is van verwerking van persoonsgegevens, doch enkel van een dienstverlening. De complexiteit van de loutere toepassing binnen het opzet van de CSD OVL en de PZ Ninove toont aan dat er op dat vlak binnen het functioneel videomodel van de GPI één en ander moet bekeken worden daar dit door zijn veelvoud aan deelname van entiteiten en systemen veel complexer is. Ten overvloede herhaalt het COC het gegeven dat het gaat om een suggestie annex uitnodiging tot verder onderzoek, en dus niet om een definitief standpunt.

6.4 Koppeling van systemen

64. De GPI maakt momenteel gebruik van een veelheid aan systemen, platformen en applicaties met gelijklopende mogelijkheden en finaliteiten. Daarbij is het niet altijd duidelijk wat de exacte rol is van de O365 GPI applicaties in het licht van de politionele verwerkingen *sensu lato*, noch is het duidelijk in hoeverre de GPI evolueert naar toestanden van (quasi) *vendor lock-in*⁵⁴. Het functioneel videomodel (stuk 17) biedt voldoende mogelijkheden om beeldverwerkingen binnen de eigen systemen te houden zonder een beroep te moeten doen op externen. De GPI zal een keuze moeten maken inzake de exacte rol die de O365 GPI applicaties dienen te spelen – tot zelfs of ze überhaupt wel een rol moeten spelen - in het licht van de eigen systemen inzonderheid FOCUS, alsmede welke verantwoordelijkheden daarmee gepaard gaan op het vlak van (functioneel) verwerkingsverantwoordelijke, verwerker en leverancier (cf supra punt 6.3).

6.5 Beheer van toegangen

65. De diversiteit aan beheersystemen zoals LDAP, PolBacc, ACC, LORI, Active Directory tot zelfs beheer van toegangen in bepaalde applicaties zelf en hun onderlinge verhouding bemoeilijkt een toegangsbeheer in de zin van de Ministeriële richtlijn. Gekoppeld aan een diversiteit van systemen voor het beheer van de logbestanden tot zelfs het ontbreken ervan in bijvoorbeeld *MS Teams* of met het oog op de controle van de rol die leveranciers/verwerkers opnemen, kan niet anders dan vastgesteld worden dat het beheer en de audit van toegangen dringend in lijn met de Ministeriële richtlijnen dient te worden gebracht, en dit op het vlak van:

- de rol van de bron voor het personeelsbeheer van de geïntegreerde politie en de wijze waarop dit in de individuele diensten van de federale politie of zones van de lokale polities wordt gematerialiseerd alsmede de afgeleide processen zoals het telefoonregister CRC en de emailadressen police.belgium.eu;
- het beheer van toegangen binnen een applicatie zelf;
- het onderscheid tussen medewerkers intern (Ops/CaLog) en medewerkers extern aan de GPI evenals alle externe partijen die gebruik maken van informatie van de politie;

⁵³ Vgl. HvJ 5 december 2023, C-683/21, r.o. 41 – 45.

⁵⁴ Het begrip *Vendor lock-in* verwijst naar de afhankelijkheid van een afnemer bij een leverancier voor bepaalde producten en/of diensten, omdat de afnemer niet in staat is om van leverancier (in kwestie) te veranderen zonder substantiële kosten of (operationele) ongemakken.

- de controle en de audit hierop.

Inzonderheid met betrekking tot *MS Teams* stelt het COC de awareness vast bij de PZ Ninove en de CSD OVL op het vlak van het ontbreken van logbestanden, alsmede het engagement om daar met de bevoegde directie aan te werken.

Het COC roept de betrokken partijen dan ook op dit verder uit te klaren en te remediëren.

6.6 Impact- en risicoanalyses – hergebruik van de gegevensbeschermingseffectbeoordeling

66. Ongeacht het schrappen van de principiële toestemming van de gemeenteraden voor het gebruiken van mobiele camera's (cf. artikel 25/4 §6 WPA) door de politiediensten, dienen in de context van het politieel cameragebruik nog steeds impact- en risicoanalyses te worden uitgevoerd, zowel op operationeel vlak als op het vlak van de bescherming van de persoonlijke levenssfeer. Wat deze laatste betreft preciseert dit document tevens per type mobiele camera de doeleinden waarvoor de camera's zullen worden geïnstalleerd of gebruikt, evenals de gebruiksmodaliteiten ervan. In zoverre een gegevensbeschermingseffectbeoordeling (*DPIA*) dient te worden verricht conform artikel 58 WVG, spreekt het voor zich dat daarvoor ook hetzelfde document kan worden gebruikt.

Belangrijk is om te benadrukken dat het **niet** de bedoeling is van een risico- en impactanalyse op het vlak van de bescherming van de persoonlijke levenssfeer, zoals voorzien in de WPA⁵⁵ of een *DPIA* zoals voorzien in de WVG⁵⁶, om puur operationele en strategische zaken te vermelden of te analyseren in functie van de risico's, laat staan om dergelijke zaken voor te leggen aan de gemeenteraad indien zulks voorzien is in de wet. In het raam van de toestemmingsaanvraag stelt de wetgever duidelijk dat deze gebaseerd moet zijn op een impact- en risicoanalyse. Met andere woorden, het is een denkoefening over de beginselen van proportionaliteit en subsidiariteit, en door deze analyse uit te voeren, zullen de doeleinden en de categorieën van verwerkte gegevens duidelijk bepaald worden. Hierdoor zal de verwerkingsverantwoordelijke ook het soort camera's en de bewaringsduur kunnen evalueren die nodig zijn om de operationele doelstellingen te bereiken. Wanneer dus de verwerkingsverantwoordelijke deze oefening heeft gemaakt, en voor het cameragebruik waarvoor de wet vereist dat er een principiële voorafgaandelijke toestemmingsaanvraag wordt gericht aan de bevoegde overheid, volstaat een vermelding *in abstracto* van de resultaten van deze analyse aan deze bevoegde overheid, zodat er enerzijds niets de openbaarheid ervan in de weg staat, maar anderzijds ook geen operationele en/of tactische en/of strategische elementen worden openbaar gemaakt.

Evenzeer geldt dat één enkele gegevensbeschermingseffectbeoordeling zou kunnen worden gebruikt om meerdere verwerkingen die vergelijkbaar zijn in termen van aard, omvang, context, doel en risico's te beoordelen. Dit kan zeker in het geval, waarbij een functioneel videomodel voor de geïntegreerde politie, al dan niet gedeeltelijk, wordt geïmplementeerd hetzij nationaal, hetzij arrondissementeel.

6.7 Testen van politieele verwerkingen – noodzaak zonder wettelijk kader

67. Het COC begrijpt de bijzondere toestand van het samengaan van de noodzakelijke ontwikkelingen en het testen ervan in een context van politieele verwerkingen. De middels de wet van toepassing zijnde ISO27K normen ter zake⁵⁷ stellen dat "*development, test and operational environments must be separated*". Het COC kan niet anders dan, *hic et nunc*, de afwezigheid vaststellen van een regelgevend kader omtrent het gebruik van operationele gegevens voor het ontwikkelen en testen van nieuwe gegevensverwerkingssystemen binnen een context van de politieele verwerkingen van bestuurlijke en gerechtelijke politie, maar begrijpt in deze ten volle de noodzaak. Het ontwikkelen van een wetgevend initiatief hieromtrent is dit evenzeer en wordt stilaan urgent gezien de nakende volledige implementatie van de AI Act (Verordening Artificiële Intelligentie⁵⁸).

⁵⁵ Art 25/4 §2 WPA.

⁵⁶ Art 58 WVG.

⁵⁷ ISO 270001 A.12.1.4

⁵⁸ Verordening (EU) 2024/1689 van het Europees Parlement en de Raad van 13 juni 2024 tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie en tot wijziging van de Verordeningen (EG) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013, (EU) nr. 2018/858, (EU)

6.8 Samenvattend

68. Samenvattend suggereert het Controleorgaan om bij de politionele verwerkingen van camerabeelden :

- te werken aan een normatief kader dat uitgaat van politionele verwerkingen en niet noodzakelijk van politionele gegevensbanken;
- de relaties tussen de verschillende actoren met name (functioneel) verwerkingsverantwoordelijke, verwerker en leverancier op het vlak van de verantwoordelijkheid van de verwerkingen te bepalen;
- de ministeriële richtlijnen in uitvoering van de bepalingen van art 44/4 WPA daadwerkelijk als normen te gebruiken en de verwerkingen daarop af te stemmen, inzonderheid binnen het functioneel videomodel;
- het hergebruik van gegevensbeschermingseffectbeoordelingen door verschillende verwerkingsverantwoordelijken te bekijken;
- een regelgevend kader te ontwikkelen voor het testen van politionele verwerkingen met behulp van operationele gegevens.

OM DEZE REDENEN, het Controleorgaan;

verzoekt de beleidsverantwoordelijken rekening te houden met de in dit rapport geformuleerde suggesties.

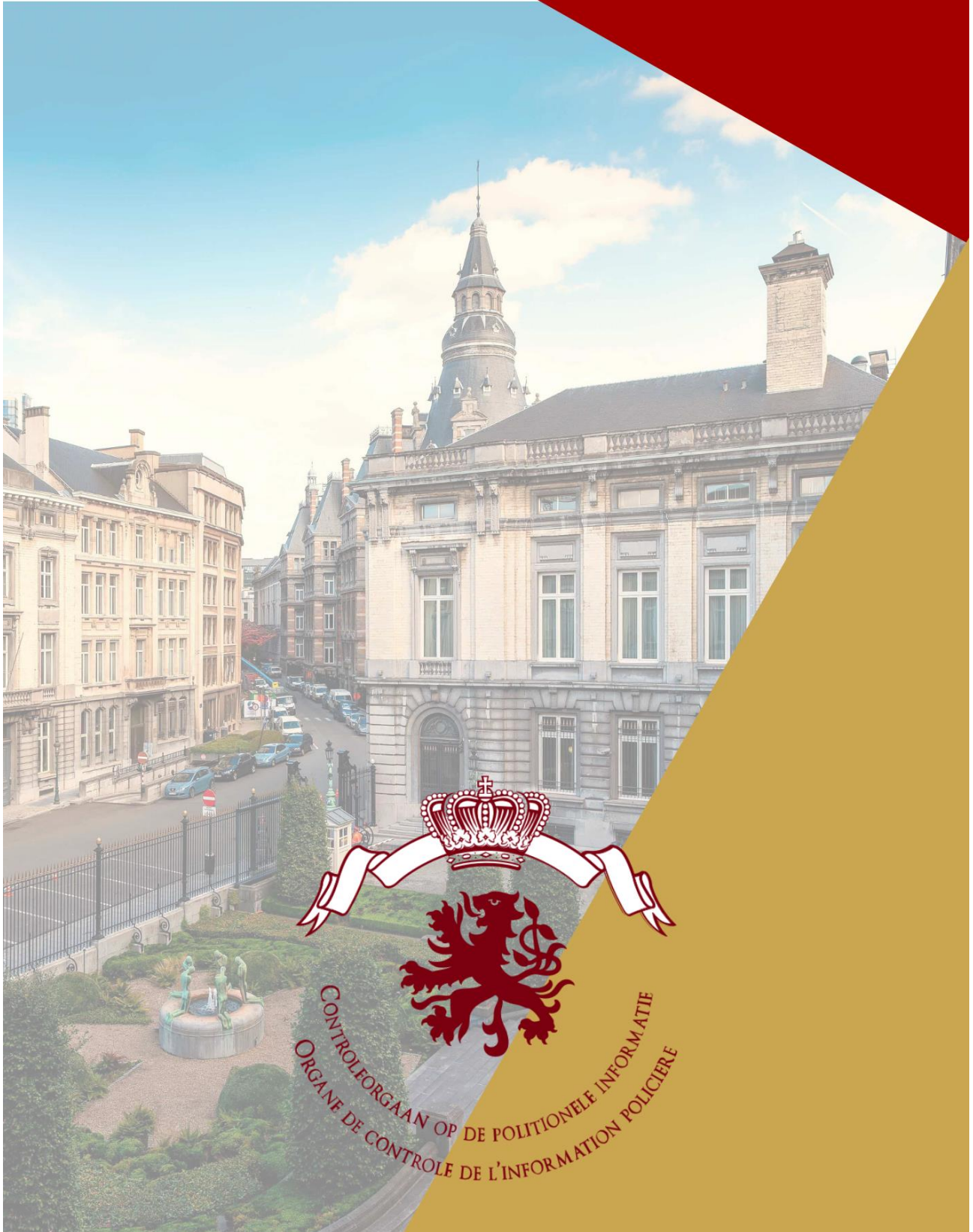
Aldus goedgekeurd door het Controleorgaan op de Politionele Informatie op 31 oktober 2025.

Afschrift aan:

- De korpschef van de PZ Ninove
- De directeur-coördinator van het arrondissement Oost Vlaanderen
- De Minister van Binnenlandse Zaken
- De Minister van Justitie
- De commissaris-generaal
- De Voorzitter van de Vaste Commissie van de Lokale Politie

Voor het Controleorgaan,

Frank SCHUERMANS
Voorzitter *a.i.* (GET)



CONTROLEORGaan OP DE POLITIONELE INFORMATIE
ORGANE DE CONTROLE DE L'INFORMATION POLICIERE

