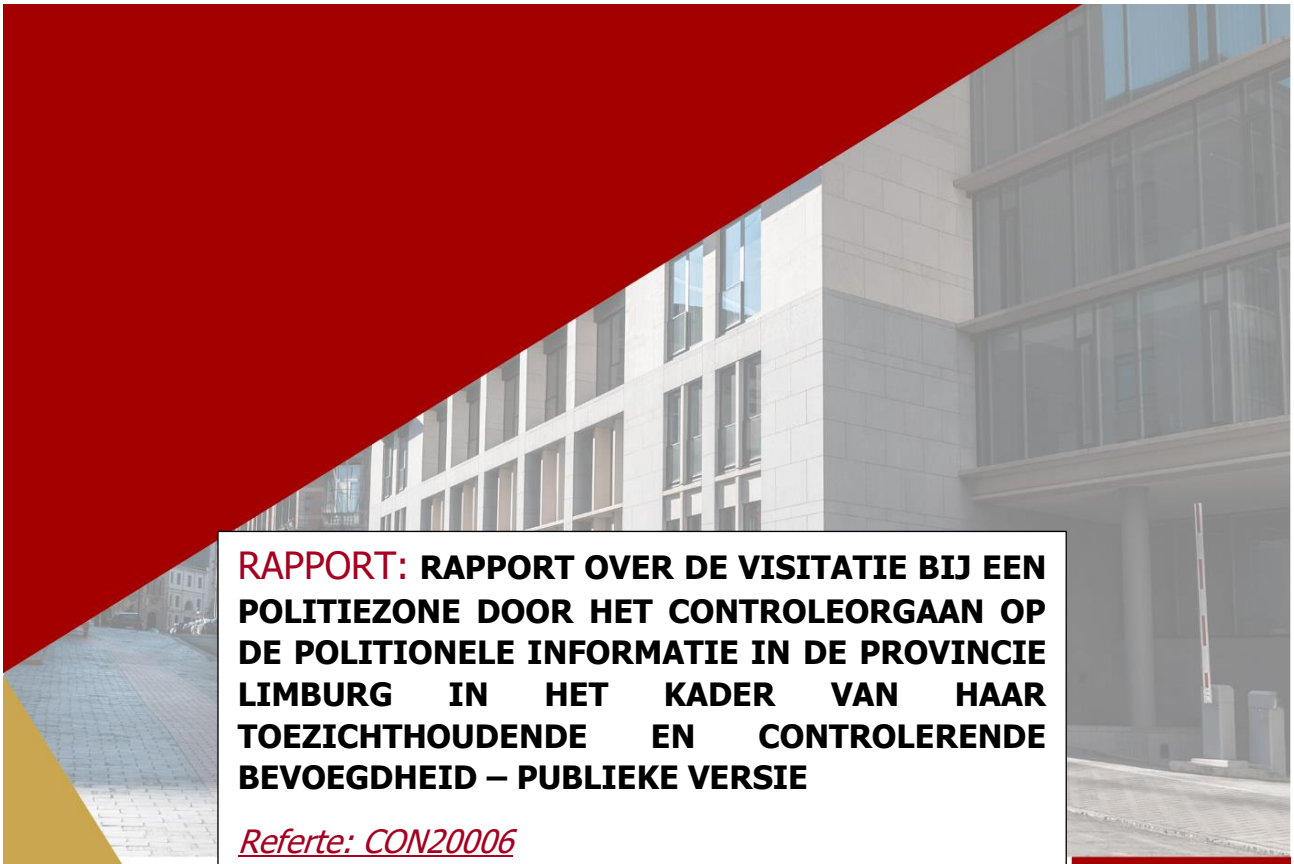


RAPPORT: **RAPPORT OVER DE VISITATIE BIJ EEN POLITIEZONE DOOR HET CONTROLEORGAAN OP DE POLITIONELE INFORMATIE IN DE PROVINCIE LIMBURG IN HET KADER VAN HAAR TOEZICHTHOUDENDE EN CONTROLERENDE BEVOEGDHEID – PUBLIEKE VERSIE**

Referte: CON20006

INHOUDSOPGAVE

RAPPORT

SYNTHESE VAN DE VISITATIE[1]

Voorwerp en opzet van het onderzoek

Op 28 oktober 2020 heeft het Controleorgaan een globale visitatie uitgevoerd bij een lokale politiezone in de provincie Limburg. Met de visitatie wordt uitvoering gegeven aan het Strategisch Plan van het Controleorgaan waarbij wordt gestreefd om jaarlijks een aantal politiezones en entiteiten van de federale politie te bezoeken met het oog op de uitvoering van zijn controle- en onderzoeksbevoegdheden. Het toezicht bij de politiezone was een spontane visitatie. De visitatie was dus niet het gevolg van een (individuele) klacht of het gevolg van het bestaan van (concrete) aanwijzingen over het niet naleven van de wet- en regelgeving door de gevisiteerde lokale politie.
Er werd geopteerd om een visitatie in de breedte uit te voeren. Dit betekent dat de visitatie betrekking had op meerdere thema's zonder al te diepgaand op de verschillende thema's in te gaan. Daarbij werd in het bijzonder aandacht besteed aan de toepassing van het juridisch kader inzake gegevensbescherming.

De visitatie omvatte vijf thema's:

1) het gebruik van camera's;
2) het beheer van de gegevens en informatie in de ANG;
3) bijzondere gegevensbanken;
4) controlesystemen van het personeel;
5) informatieveiligheid: organisatie, beleid en ICT-beheer.

Onderzoeksbevindingen

De politie van beschikt over een beperkt aantal vaste camera's die gericht zijn op de publieke ruimte, drie vaste *ANPR* camera's en één mobiele *ANPR*-camera. Opvallend was dat de politiezone niet meteen een antwoord kon geven op de vraag wie precies de verwerkingsverantwoordelijke is voor de 2 vaste ANPR-camera's aan de grensovergang met Nederland. Uit het onderzoek blijkt evenwel dat de politiezone wel degelijk de verwerkingsverantwoordelijke is voor deze 2 *ANPR*-camera's, ook al worden de beelden niet door de PZ bewaard, maar door de (arrondissementele directie van de) federale politie. Wat betreft de vaste camera's van de politie die toezicht houden op de openbare ruimte en de mobiele *ANPR* (zichtbaar cameragebruik) was geen toestemming van de gemeenteraad gevraagd waardoor deze niet wetsconform worden gebruikt. De toestemming van de gemeenteraad werd pas op 24 november 2020 verleend, dus na datum van de visitatie, en op 18 januari 2021 aan het Controleorgaan bezorgd.

Op het moment van de visitatie gebeurde de toegang tot de camerabeelden op basis van een algemene (dienst)login, wat niet in overeenstemming is met de wettelijke verplichtingen. Er wordt geen gebruik gemaakt van een individualiseerbare toegang tot de (*ANPR*)-camerabeelden en er kan geen controle op het logbestand van de mobiele *ANPR*-camerabeelden uitgevoerd worden, wat nochtans wettelijk verplicht is. De politiezone beschikte ook niet over een (concreet) uitgewerkt toegangs- en gebruikersbeheer inzake cameragebruik. Dezelfde vaststelling geldt voor de oprichting van de lokale technische gegevensbank voor de *ANPR*-beelden, die door de PZ op een laptop worden bewaard en daardoor als een 'technische gegevensbank' moet worden beschouwd. Er was voorafgaand aan het gebruik van de mobiele *ANPR* bovendien geen *DPIA,* noch werd het advies van de *DPO* opgemaakt vóór de oprichting van een lokale technische gegevensbank. De politiezone beschikte evenmin over een register van cameragebruik.

De politiediensten verwerken ook persoonsgegevens voor niet-politionele doeleinden. In dat geval is naast de WGB[2] ook de AVG van toepassing. In dat verband maakt de PZ ook gebruik van politionele camerabeelden of digitale gegevens met het oog op het behandelen van klachten of controle op de naleving van de arbeidsvoorwaarden (wat betreft het gebruik van door de PZ ter beschikking gestelde netwerkfaciliteiten). Voor deze laatste hanteert de PZ een procedure die een afspiegeling of analoge toepassing is van de principes van de collectieve arbeidsovereenkomst (CAO) nr. 81 met betrekking tot de controle op het gebruik van het internet. Voor het COC is die basishouding zonder meer een *best*

[1] Een publieke versie van een rapport betekent dat deze niet noodzakelijk alle elementen bevat die vermeld worden in het basisrapport dat een de bestemmelingen wordt gericht. Sommige elementen of passages zijn weggelaten of werden geanonimiseerd. Daar kunnen diverse redenen voor zijn, zowel van wettelijke aard of omwille van opportuniteitsmotieven: het niet openbaren van politionele technieken of tactieken, het geheim van het onderzoek, het beroepsgeheim, het feit dat inmiddels werd geremedieerd aan een tekortkoming, enz…
[2] De wet van 30 juli 2018 "*betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens*".

practice. Hoewel deze controles slechts uitzonderlijk plaatsvinden, kan dat de PZ er niet van weerhouden om ter zake een *policy* op te maken waarin de procedure, de gevolgen en de rechten van het politiepersoneel worden uitgewerkt. Dat geldt eveneens voor het gebruik van politionele camerabeelden voor de controle op de naleving van de arbeidsvoorwaarden van het personeel.

Met betrekking tot het informatiebeheer kon een zeer goede werking worden vastgesteld. Voorafgaand aan de flux naar de Algemene Nationale Gegevensbank (hierna 'ANG') gebeurt er een kwaliteitscontrole van de gegevens. Op het vlak van de correlatie van de ANPR beelden met nationale lijsten wordt de optie 32[3] uitgevoerd door de Politiezone HANO. Dit impliceert evenwel dat het gebruik van de *blacklists* of nationale lijsten niet wordt gelogd voor de PZ. Het gevolg is dat er een transfer plaatsvindt op een wijze die op moment van redactie van dit rapport nog dient verduidelijkt te worden door de PZ.

De PZ maakt gebruik van bijzondere gegevensbanken die in het register van verwerkingen worden geregistreerd. Bepaalde van deze gegevensbanken kunnen echter bezwaarlijk als bijzondere gegevensbanken worden beschouwd.

De politiezone heeft een functionaris voor de gegevensbescherming (*DPO*), op basis van een provinciaal samenwerkingsverband. De *DPO* beschikt over de vereiste competenties en oefent de functie voltijds uit, maar verdeeld haar werkzaamheden over 14 politiezones. Hoewel een samenwerkingsverband van DPO's daadwerkelijk een meerwaarde kan zijn en door het COC wordt toegejuicht, werd vastgesteld dat, door het grote aantal politiezones dat onder het werkveld van de DPO valt, de DPO moeilijk haar opdrachten daadwerkelijk en efficiënt kan uitvoeren. Gelet op de beperkte tijdsbesteding, kan de DPO evenmin proactief het beleid inzake gegevensbescherming en informatieveiligheid opvolgen.

De aspecten van informatieveiligheid, gegevensbescherming en ICT worden in principe minstens jaarlijks geëvalueerd (onder leiding van de korpschef). Aan deze vergaderingen wordt deelgenomen door de lokale coördinator/contactpersoon voor gegevensbescherming en de *DPO*. Tijdens de visitatie werd daarvan geen rapportering aan het COC voorgelegd. Daarnaast diende de politiezone reeds onder de toepassing van het uitvoeringsbesluit van 6 december 2015 over een informatieveiligheidsplan te beschikken dat op het moment van de visitatie nog niet was opgemaakt.

Een aantal maatregelen werden geïmplementeerd om de integriteit, confidentialiteit en continuïteit van informatie en informatiesystemen te garanderen. Deze maatregelen worden echter niet structureel nagekeken. Interne controles en *self-assessments* met betrekking tot ICT veiligheid worden niet regelmatig uitgevoerd (bijvoorbeeld door met periodieke kwetsbaarheidsscans proactief de gaten in de beveiliging van IT-systemen en software op te sporen). Er werden de voorbije jaren ook geen externe beveiligingsaudits uitgevoerd.

Er worden geen proactieve controles op de logbestanden uitgevoerd; dit gebeurt enkel op vraag. Er is geen formeel ICT continuïteitsplan gedefinieerd binnen de ICT dienst. Desalniettemin zijn er acties ondernomen vanuit de ICT dienst van de politiezone om de beschikbaarheid van de digitale gegevens en de informatie-verwerkende faciliteiten te garanderen.

Conclusie – aanbevelingen – corrigerende maatregelen

Conclusie

Slechts een gering aantal aspecten van de gecontroleerde thema's blijken in overeenstemming met de wetgeving. Wat betreft de aspecten met een duidelijke dominantie op het vlak van gegevensbescherming, blijkt dat de PZ wel de ambitie heeft om antwoord te kunnen bieden op bepaalde gevoelige aangelegenheden, maar dit gedeeltelijk werd belemmerd door de geringe effectieve tijdsbesteding enerzijds en het gebrek aan uitvoerige documentatie betreffende de daarmee samenhangende aspecten anderzijds (ICT en informatieveiligheid), niettegenstaande het overduidelijk engagement bij de aangestelde personeelsleden en de *DPO*.

[3] Zie voetnoot 67.

Voorgaande algemene vaststelling weerspiegelt de concrete vastgestelde tekortkomingen. Vooral op het domein van het gebruik van camerabewaking en de toepassing van het wettelijk kader met betrekking tot het gegevensbeschermingsrecht moeten er nog verschillende stappen worden genomen. Daarentegen heeft de PZ een zeer goede werking van het functioneel beheer.

Hoewel er een aantal korpsrichtlijnen met betrekking tot informatieveiligheid werden opgesteld, heeft de PZ geen risico-gestuurd algemeen informatieveiligheids- en continuïteitsplan waarbinnen de organisatie, en in het bijzonder de ICT dienst, haar eigen maatregelen kan kaderen. Zo'n risico-gebaseerde aanpak zou toelaten om de genomen maatregelen te evalueren, te formaliseren en te documenteren. De ICT dienst van de PZ voorziet in een reeks ICT beveiligingsinitiatieven, maar het periodiek (intern/extern) nazicht van de goede werking en de volledigheid van deze initiatieven gebeurt niet op een structurele en formele wijze. De betrokkenheid van de DPO bij het opvolgen, bijsturen en implementeren van het informatieveiligheids- en gegevensbeschermingsbeleid dient verhoogd te worden. Een structurele aanpak en periodieke opvolging zijn hier aangewezen.

Bijgevolg dringen een reeks aanbevelingen zich op die moeten bijdragen tot een verbetering van de efficiëntie en effectiviteit van de (persoons)gegevensverwerking door de PZ.

De vastgestelde wettelijke tekortkomingen nopen het Controleorgaan echter ook tot het nemen van corrigerende maatregelen waarbij de PZ zich binnen een welbepaald tijdspanne moet regulariseren.

Verzoek

Het Controleorgaan verzoekt dat de korpschef, in afwachting van het uitvoeringsbesluit inzake het lokaal cameraregister, een lokaal register van het cameragebruik aanlegt of in een afzonderlijk luik in het register van verwerkingen opneemt waarin de types van camera's, de doeleinden en het opslagmedium van de beelden duidelijk worden vermeld.

Aanbevelingen

1) Aanbeveling
Met het oog op een effectieve en efficiënte toepassing van de *ANPR*-verwerkingen is het van belang dat de PZ een duidelijk interventiebeleid voor de hits op nationale lijsten en een duidelijk actie- en interventiebeleid op de lokale lijsten uitwerkt.

2) Aanbeveling
Het Controleorgaan dringt er op aan dat een *policy*/beleid wordt opgesteld dat het mogelijk maakt een efficiënt mechanisme in plaats te stellen waarbij een continue monitoring gebeurt van de profielen en toegangen in real time kunnen beheerd worden in functie van de reële personeelsbezetting.

3) Aanbeveling
Het COC dringt er op aan dat de PZ in een korpsnota een beleid uitstippelt voor het aanleggen van bijzondere gegevensbanken waarin parameters zijn opgenomen op basis waarvan kan afgetoetst worden of het aanleggen van een bijzondere gegevensbank voor die welbepaalde verwerkingsactiviteit beantwoordt aan de wettelijke voorwaarden van artikel 44/11/3 WPA.

4) Aanbeveling
Het is van belang dat de korpschef in het korpsorder duidelijk onderscheid maakt tussen de diverse aspecten die worden beoogd op het vlak van de toegang tot en het gebruik van het internet en van sociale media voor persoonlijke en professionele doelstellingen en al dan niet gebruik van persoonlijke toestellen[4]. Zo moet de toegang tot het internet (zoekopdrachten, toegelaten en verboden websites) tijdens de diensturen worden onderscheiden van het gebruik van sociale media tijdens de diensturen voor persoonlijke doeleinden, enerzijds, en voor zover politionele informatie zou kunnen gedeeld worden, anderzijds. In een apart luik of afzonderlijk document wordt het gebruik van mobiele privétoestellen voor operationele doeleinden en het gebruik van professionele mobiele toestellen voor persoonlijke doeleinden (afzonderlijk) beschreven. Het is daarbij van belang dat het document duidelijk beschrijft wat toegelaten of

[4] Het Controleorgaan vestigt daarbij de aandacht op wettelijke regelingen die de vertrouwelijkheid van privécommunicatie beschermen, zoals artikel 314bis van het Strafwetboek en de wet van 13 juni 2005 "*betreffende de elektronische communicatie*" die de vertrouwelijkheid van de telecommunicatie beschermt (artikel 5 van deze wet).

verboden is, in welke omstandigheden en onder welke voorwaarden controle kan uitgevoerd worden, wat de gevolgen zijn wanneer inbreuken op het document worden vastgesteld en wat in dat verband de rechten van de betrokkene zijn. Het is dus van belang dat een duidelijk onderscheid wordt gemaakt tussen de diverse aspecten en doeleinden waarbij een procedure wordt uitgetekend waarin de basisprincipes van transparantie en rechten van de betrokkene concreet worden uitgewerkt. Dat is eveneens het geval wat betreft het gebruik van operationele camerabeelden voor de controle op de naleving van de arbeidsvoorwaarden.

5) Aanbeveling
Het COC dringt aan op een bijsturing van de tijdsbesteding voor de *DPO* en het beperken van het aantal politiezones waarvoor zij als *DPO* een coördinerende rol heeft, tenzij de assistent-*DPO's* daadwerkelijk hun taak op een zelfstandige wijze kunnen uitoefenen. Het COC is van oordeel dat de *DPO* in de huidige omstandigheden niet over voldoende middelen (tijd) kan beschikken om de taken van een *DPO* adequaat uit te voeren voor het grote aantal politiezones waarvoor zij aangesteld is.

6) Aanbeveling

Het wordt aanbevolen de volgende actiepunten op te nemen in het informatieveiligheidsplan:

- de verdere uitwerking en verfijning van het beleid inzake informatieveiligheid en gegevensbescherming via korpsrichtlijnen en procedures. Dit beleid moet regelmatig door het management gerevalueerd worden zodat het relevant blijft, in lijn met de realiteit. Het is hierbij belangrijk om de uitgewerkte korpsnota's en procedures te communiceren, te duiden en regelmatig te herhalen (door middel van bewustmakingscampagnes);
- maturiteitsmetingen, risico- en kwetsbaarheidsanalyses zijn belangrijke pijlers in het beveiligingsbeleid en dragen bij tot een optimale risico-gebaseerde informatieveiligheid. De tijdsbesteding van de *DPO* is ook een onderdeel van dit risicobeheer;
- het opzetten van formele overleg- en communicatieprocedures met alle betrokken partijen **binnen de PZ** zodoende dat de *DPO* meer bij de werkzaamheden van de organisatie betrokken wordt en steeds over de nodige informatie beschikt voor de uitvoering van de opdracht die hem toevertrouwd werd.

7) Aanbeveling
Het is aanbevolen om een risicoanalyse uit te voeren m.b.t. het beheer van logbestanden en het monitoren van de interne ICT-systemen teneinde de nodige garanties te bekomen rond de traceerbaarheid van gegevensverwerkende activiteiten.

8) Aanbeveling
Het COC dringt er op aan om:

- uitsluitend het gebruik van nominatieve/individuele gebruikersaccounts toe te laten in het kader van het operationeel beheer. Het gebruik van een generiek gebruikersaccount voor systeembeheer dient sterk gelimiteerd te worden en wordt enkel toegelaten indien dit technisch vereist is;
- alle geprivilegieerde accounts te inventariseren, inclusief domein- en lokale accounts, om er zeker van te zijn dat alleen geautoriseerde personen verhoogde rechten hebben;
- ervoor te zorgen dat alle gebruikers met toegang tot een geprivilegieerde account een speciale of secundaire nominatieve account gebruiken voor het uitvoeren van ICT activiteiten waarvoor verhoogde rechten nodig zijn. Dit geprivilegieerde account mag alleen worden gebruikt voor deze administratieve activiteiten en niet voor het uitvoeren van de dagdagelijkse operationele activiteiten, surfen op het internet, e-mail of soortgelijke activiteiten;
- alle activiteiten m.b.t. het gebruik en het beheer van deze geprivilegieerde accounts op te nemen in logbestanden en integriteitsbeschermende maatregelen voor deze logbestanden te voorzien.

9) Aanbeveling
De PZ wordt aangespoord tot het versterken van toezicht en controles teneinde te kunnen beschikken over een correct en actueel inzicht in de werking en effectiviteit van de integrale informatiebeveiliging. Dit houdt onder meer in:

- het toezien op het naleven van wettelijke, regelgevende en contractuele verplichtingen alsook van de eigen beleidslijnen met betrekking tot informatieveiligheid en in het bijzonder de verwerking van persoonsgegevens;
- het regelmatig controleren of de informatiesystemen in overeenstemming zijn met de normen voor de tenuitvoerlegging van de beveiliging en het meten van de technische conformiteit. Dit kan onder meer door het uitvoeren van *vulnerability scans*, *penetration testing* en *security audit/review*;
- een periodieke doorlichting uitgevoerd door een onafhankelijke derde partij is een absolute meerwaarde.

10) Aanbeveling
Het is aanbevolen een ICT noodvoorzieningsplan (*DRP* of *Disaster Recovery Plan*) en continuïteitsplan voor alle kritieke processen en essentiële informatiesystemen van de organisatie op te stellen en om dit op periodieke basis te testen. Een *DRP* voor ICT gaat veel verder dan louter een *back-up* voorzien. Hoe bereid je de organisatie voor op alle mogelijke calamiteiten die de ICT-systemen kunnen ondervinden, is de te stellen vraag

Corrigerende maatregelen

Gelet op artikel 221 § 1, en 247, 4°,5° en 6° WGB;

Gelast de PZ:

a) om de toegang tot de camerabeelden in overeenstemming te brengen met artikel 25/7 § 1, derde lid WPA, zodat de reden van de bevragingen geregistreerd wordt. Het bewijs van deze wetsconforme implementatie wordt binnen de negen maanden na datum van kennisname van deze corrigerende maatregel aan het Controleorgaan overlegd;

b) om de logbestanden van de toegang tot de camerabeelden overeenkomstig artikel 56 WGB bij te houden. Het bewijs van deze wetsconforme implementatie wordt binnen de negen maanden na datum van kennisname van deze corrigerende maatregel aan het Controleorgaan overlegd;

c) om de criteria voor opname op de lokale *ANPR* lijsten te verduidelijken en binnen de drie maanden na datum van kennisname van deze corrigerende maatregel aan het Controleorgaan over te maken;

d) om op regelmatige basis loggings op te vragen van de ANG en proactieve controles door middel van steekproeven (2 x/jaar) te houden met het doel toezicht te houden op het verplicht ingeven van een reden van raadpleging en op eventuele onrechtmatige consultaties en dit een eerste maal binnen de zes maanden na kennisname van deze corrigerende maatregel en de resultaten ervan ter beschikking te houden van het COC

e) om een informatieveiligheidsplan op te maken. Het informatieveiligheidsplan wordt binnen de negen maanden na datum van kennisname van onderhavig rapport ter beschikking gesteld van het Controleorgaan;

Zegt voor recht dat de aanvangsdatum van de corrigerende maatregelen en de datum van kennisname ervan bedoeld onder de littera a) tot en met e) moet begrepen worden als zijnde de datum van het overmaken van het huidig definitief rapport van het Controleorgaan per e-mail tegen ontvangstbevestiging vermeerderd met twee dagen.

Het Controleorgaan wijst op de mogelijkheid voor de partijen om binnen de dertig dagen na de beslissing van het Controleorgaan beroep aan te tekenen bij het hof van beroep van de woonplaats of zetel van eiser (artikel 248 § 1, eerste lid en § 2 WGB).

RAPPORT

1. INLEIDING

1.1. De bevoegdheden van het Controleorgaan

1. De wet van 30 juli 2018 *betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens* (hierna 'WGB')[5] heeft het Controleorgaan op de politionele informatie ('Controleorgaan' of 'COC') hervormd tot onder meer een volwaardige toezichthoudende autoriteit bovenop de bestaande controlerende bevoegdheden inzake politionele informatiehuishouding zoals voorzien in de Wet van 5 augustus 1992 op het Politieambt (hierna 'WPA'). In artikel 71 § 1 en de hoofdstukken 2 en 3 van titel VII van de WGB worden de opdrachten en de bevoegdheden van het COC omschreven. Daarbij wordt tevens verwezen naar de controleopdrachten vervat in de artikelen 44/1 tot en met 44/11/13 WPA inzake de informatiehuishouding van de politiediensten. Op die manier heeft het Controleorgaan een toezichthoudende en een controlerende opdracht. Dit betekent dat, naast privacy en gegevensbescherming, het COC ook aandacht heeft voor elementen als efficiëntie en effectiviteit van het politieoptreden.

Het Controleorgaan is bevoegd voor de politiediensten[6], de Algemene inspectie van de federale en lokale politie (AIG)[7] en de Passagiersinformatie-eenheid (PIE)[8]. De toezichtbevoegdheid van het Controleorgaan wat betreft de politiediensten omvat zowel de operationele als niet-operationele verwerkingsactiviteiten[9]. Daarnaast is het Controleorgaan tot slot ingevolge artikel 281 § 4 van de algemene wet van 18 juli 1977 "*inzake douane en accijnzen*", ten aanzien van de Dienst Geschillen van de Algemene Administratie van Douane en Accijnzen bevoegd in het kader van de vorderingen gericht aan de PIE in fiscale materies.

Wat de controleopdracht betreft, is het Controleorgaan belast met de controle van de verwerking van de informatie en de gegevens bedoeld in artikel 44/1 WPA, met inbegrip van deze ingevoegd in de gegevensbanken bedoeld in artikel 44/2, en elke andere opdracht die haar door of krachtens andere wetten wordt verleend.

Het Controleorgaan is in het bijzonder belast met de controle van de naleving van de regels inzake de rechtstreekse toegang tot de Algemene Nationale Gegevensbank (ANG) en de rechtstreekse bevraging ervan, alsook van de naleving van de in artikel 44/7, 3e lid WPA bedoelde verplichting, voor alle leden van de politiediensten, tot voeding van deze gegevensbank.
Het Controleorgaan gaat door middel van onderzoek naar de werking na of de inhoud van de ANG en de procedure voor de verwerking van de daarin bewaarde gegevens en informatie overeenkomen met het bepaalde in de artikelen 44/1 tot 44/11/13 WPA en met hun uitvoeringsmaatregelen.

In het kader van het gebruik van niet-zichtbare camera's fungeert het Controleorgaan als een soort 'BAM-commissie'[10]. Overeenkomstig 46/6 WPA moet elke toestemming en verlenging voor niet-zichtbaar gebruik van camera's in de gevallen bedoeld in artikel 46/4 worden meegedeeld aan het Controleorgaan, behalve wanneer het gebruik van camera's wordt uitgevoerd onder het gezag van een magistraat. Daarbij moet het Controleorgaan onderzoeken of voldaan is aan de voorwaarden voor de beslissing, de verlenging of de uitvoering van de maatregel.

Daarnaast neemt het Controleorgaan kennis van klachten en beslist het over de gegrondheid ervan[11]. In dat verband beschikken de leden van het Controleorgaan en de leden van de dienst onderzoeken over onderzoeksbevoegdheden en kunnen corrigerende maatregelen worden genomen[12].

---

[5] *BS,* 5 september 2018. Deze wet bevat tevens bepalingen die uitvoering geven aan Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en het vrije verkeer van die gegevens en tot intrekking van de Richtlijn 95/46/EG (algemene verordening gegevensbescherming), hierna de AVG, en de Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.
[6] Zoals gedefinieerd in artikel 2, 2° van de wet van 7 december 1998 tot organisatie van een geïntegreerde politie, gestructureerd op twee niveaus (art. 26, 7°, a, WGB).
[7] Zoals gedefinieerd in artikel 2 van de wet van 15 mei 2007 op de Algemene Inspectie houdende diverse bepalingen betreffende de rechtspositie van sommige leden van de politiediensten (art. 27, 7°, d WGB).
[8] Zoals bedoeld in hoofdstuk 7 van de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens (art. 26, 7°, f WGB).
[9] Art. 4 § 2, derde lid, wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit ('WOG').
[10] BAM staat voor 'Bijzondere Administratieve Methoden'.
[11] Art. 240, 4°, WGB.
[12] Art. 244 en 247 WGB.

Tegen bepaalde beslissingen van het Controleorgaan staat binnen de dertig dagen een jurisdictioneel beroep open bij het Hof van Beroep van de woonplaats of de zetel van de eiser, die de zaak behandelt zoals in kort geding overeenkomstig de artikelen 1038, 1040 en 1041 van het Gerechtelijk Wetboek[13].

1.2. Doelstellingen

2. Het toezicht beoogt inzicht te krijgen in de toepassing van het wettelijk kader met betrekking tot de verwerking van persoonsgegevens enerzijds en de aandacht van de gecontroleerde entiteit inzake informatieveiligheid anderzijds. Bij de controlebevoegdheid staat eerder de naleving van de werkprocessen en procedures centraal. Niettemin hebben beide bevoegdheden gemeen dat persoonsgegevens worden verwerkt.

In het licht van het voorgaande zal het aspect van de informatieveiligheid ruimer zijn dan de naleving van het wettelijk kader inzake de verwerking van persoonsgegevens en/of het informatiebeheer zoals bepaald in de WPA. Het valt immers samen met de implementatie en toepassen van standaarden en normen op het vlak van informatieveiligheid zowel op het niveau van de processen als van de systemen.

De vorm van het toezicht betreft de organisatorische aspecten: de verschillende stappen in het proces en de hiermee gepaard gaande timing. Daarbij wordt onderzocht of de verwerkingsactiviteiten beantwoorden aan het wettelijke kader van de AVG, WGB en de WPA en de vereisten inzake informatieveiligheid wat betreft de structuur, verwerkingsprocessen en systemen.

2. OPZET VAN DE VISITATIE EN METHODOLOGIE

2.1. Situering

3. Op 28 oktober 2020 heeft het Controleorgaan een visitatie uitgevoerd bij een PZ in de provincie Limburg. Met de visitatie wordt uitvoering gegeven aan het Strategisch Plan van het Controleorgaan waarbij wordt gestreefd om jaarlijks een aantal politiezones en/of entiteiten van de federale politie te bezoeken met het oog op de uitvoering van de hiervoor uiteengezette controle- en onderzoeksbevoegdheden. De visitatie was dus niet het gevolg van een (individuele) klacht of het bestaan van (concrete) aanwijzingen over het niet naleven van de wet- en regelgeving door de gevisiteerde lokale politiedienst.

Met de invoering van de AVG en de WGB heerst bij de politiediensten heel wat ongerustheid over de correcte toepassing van en vragen over het wettelijk kader. Dat blijk uit de veelheid van vragen aan het Controleorgaan, zowel op het vlak van de operationele verwerkingsactiviteiten als niet-operationele verwerkingsactiviteiten, zoals de verwerking van personeelsgegevens en de controle op de arbeidsprestatie van het personeel. Daarnaast kampen veel politiezones met de complexiteit van het in 2018 gewijzigd wettelijk kader voor het plaatsen en gebruik van camera's. Daarom was de invalshoek van de visitatie opgezet met de nadruk op *sensibiliseren*, wat betreft de toepassing van de AVG, de WGB en camerawetgeving, en *compliance based* voor wat betreft de controle op de kwaliteit van de registraties in de ANG. Deze gesplitste invalshoek staat er evenwel niet aan de weg dat het Controleorgaan gepaste maatregelen neemt en moet nemen wanneer evidente wettelijke tekortkomingen en/of inbreuken worden vastgesteld.

4. Gelet op deze complexe realiteit werd geopteerd om een visitatie in de breedte uit te voeren (globale visitatie). Dit betekent dat de visitatie betrekking had op meerdere thema's zonder al te diepgaand op de individuele thema's in te gaan. Daarbij werd in het bijzonder aandacht besteed aan de toepassing van het juridisch kader inzake gegevensbescherming in het algemeen en de informatieveiligheid in het bijzonder. Als overkoepelende factor heeft informatieveiligheid immers een impact op de integriteit, betrouwbaarheid, vertrouwelijkheid en beschikbaarheid van de gegevens voor de politie. Daarbij is een belangrijke rol weggelegd voor de functionaris voor gegevensbescherming (*DPO*, *Data Protection Officer*). Deze functie krijgt ten aanzien van de (operationele) verwerkingsverantwoordelijke een adviserende en controlerende rol toebedeeld en fungeert in dit verband als het aanspreekpunt voor het Controleorgaan.

De visitatie omvatte vijf thema's:

[13] Art. 248 WGB.

1) het gebruik van camera's;
2) controle op het beheer van de gegevens en informatie in de ANG;
3) bijzondere gegevensbanken;
4) controlesystemen van het personeel;
5) informatieveiligheid: organisatie, beleid en ICT-beheer.

2.2. Methodologie

5. De visitatie viel uiteen in twee fasen. Bij de eerste fase werd aan de politiezone een vragenlijst bezorgd om de nodige informatie en documenten in te winnen over de vijf vermelde thema's. Afhankelijk van de inhoud van de antwoorden, of het (gedeeltelijk) uitblijven ervan, werd een *shortlist* (een selectie uit de antwoorden op de vragenlijst) opgesteld. Op die manier kon het plaatsbezoek tot een minimaal tijdsbestek herleid worden.

6. De tweede fase had betrekking op het bezoek ter plaatse (de eigenlijke 'visitatie'). Deze werd opgesplitst in zeven onderdelen.

1) Rondleiding in de politiezone:
   - een overzicht van de verschillende diensten;
   - bezoek aan de dispatching voor wat betreft de verwerking van de camerabeelden;
   - de ICT-infrastructuur in het kader van de informatieveiligheid.
2) Het gebruik van camerabewaking:
   - *ANPR* camera's aan de invalswegen van de stad;
   - de camerabewaking in de stad;
   - de camerabewaking binnen het cellencomplex.
3) De gegevensverwerking in de ANG, inzonderheid:
   - logging;
   - profielen;
   - centrale validatie;
   - kwaliteitscontrole.
4) Bijzondere gegevensbanken.
5) Het gebruik van mobiele toestellen al dan niet in het kader van operationele opdrachten, inzonderheid:
   - gebruik van *laptops* of *smartphones* voor operationele opdrachten;
   - gebruik van *laptops* of *smartphones* voor niet-operationele doeleinden.
6) Het verwerken van biometrische gegevens voor niet-operationele doeleinden.
7) Controle van het register van de verwerkingen en het register inzake camerabewaking.

Daarbij werd vanuit een generieke benadering de aandacht voor informatieveiligheid tegen het licht gehouden en de actieve rol van de *DPO*.

Een aspect van de visitatie is gelegen in de tendens van het gebruik van mobiele toestellen (*smartphones*, *i-pad*, *laptops*, …) voor operationele doeleinden (punt 5). Dit kan opgesplitst worden in het gebruik van privétoestellen en door de politie ter beschikking gestelde mobiele toestellen. Met 'operationele doeleinden' wordt het gebruik van mobiele toestellen voor operationele politieactiviteiten bedoeld, zoals het nemen van foto's of kopieën van documenten, en in het verlengde daarvan operationele administratieve verwerkingen, zoals het versturen van e-mailberichten met politionele informatie.

Vervolgens werd de politiezone de mogelijkheid geboden om opmerkingen op het rapport te formuleren en/of aan te geven op welke punten ondertussen al de nodige remediërende acties werden genomen die van invloed zijn op de voorgenomen aanbevelingen en/of corrigerende maatregelen. De PZ heeft binnen de opgelegde termijn van deze mogelijkheid gebruik gemaakt. Waar relevant werd met deze opmerkingen rekening gehouden.

3. RELEVANTE WETTELIJKE EN REGLEMENTAIRE BEPALINGEN

3.1. Algemeen

7. Voor de operationele thema's die het voorwerp waren van de visitatie en het grootste deel van de visitatie beslaan, komen twee wettelijke regelingen op de voorgrond: de hiervoor besproken wet van 30 juli 2018 met betrekking tot de verwerking van persoonsgegevens (WGB) en de wet op het politieambt (WPA). Op het gebruik van camerabewaking door politiediensten is door de aanpassingswet van 21 maart 2018[14] van de WPA van toepassing sinds 25 mei 2018. De wet van 21 maart 2018 voorziet evenwel in een overgangsbepaling van 12 maanden om de politiediensten de tijd te gunnen om zich in regel te stellen met deze wetswijzigingen.

8. Wat betreft het gebruik van (privé) toestellen voor niet-operationele doeleinden geldt het algemeen wettelijk kader van de AVG en de WGB. Dat is tevens het geval wanneer, bijvoorbeeld, biometrische gegevens[15] voor niet-operationele doeleinden worden verwerkt of het gebruik van (politionele) camerabeelden voor de controle op de naleving van de arbeidsvoorwaarden van het politiepersoneel[16]. Gezien de complexiteit van politionele en niet-politionele verwerkingen wordt hierna in 3.2. eerst een korte duiding verstrekt.

3.2. Politionele en niet-politionele verwerkingsactiviteiten

9. Op het vlak van de verwerking van persoonsgegevens omvatten de taken en opdrachten van een politiedienst globaal genomen twee domeinen: politionele verwerkingen (met name bestuurlijke en gerechtelijke politie) en gewone (administratieve) of niet-politionele verwerkingen. Voorbeelden van deze laatste zijn personeelsmanagement en andere administratieve en logistieke verwerkingsactiviteiten door de politie. Op het vlak van transparantie en de rechten van de betrokkene zijn de politionele verwerkingen aan (verregaande) beperkingen onderworpen terwijl dat principieel niet het geval is voor de niet-politionele verwerkingen. Dit komt er op neer dat de controle op de politieambtenaar in het kader van de arbeidsrelatie (niet-politionele verwerking) onderworpen is aan de bepalingen van de AVG en uitvoeringsbepalingen zoals vastgelegd in titel 1 van de WGB. Voorbeelden zijn de controle op het internet- en e-mailgebruik (voor persoonlijke doeleinden), het verwerken van bijzondere categorieën van persoonsgegevens, zoals vingerafdrukken, in het kader van het personeelsbeleid en het gebruik van camerabewaking in een arbeidsrechtelijke context. Wat de verwerking van biometrische gegevens in het kader van het personeelsbeleid betreft, heeft het Controleorgaan zich reeds in verschillende dossiers op het standpunt gesteld dat in de huidige stand van de wetgeving een gepaste en afdoende wettelijke grondslag ontbreekt (zie verder rubriek 4.5.1). Op de politionele verwerkingen is, zoals hiervoor gesteld, titel 2 WGB en de WPA van toepassing[17].

10. Bij deze complexe wetgeving kan de bijstand van de functionaris voor gegevensbescherming (*DPO*) niet ontbreken. Door de WGB worden aan de *DPO* belangrijke opdrachten toebedeeld. De *DPO* levert niet alleen desgevraagd bijstand aan de (operationele) verwerkingsverantwoordelijke. Hij moet tevens toezien op de naleving van de toepasselijke wetgeving en interne regels[18]. Hij mag bijgevolg geen afwachtende houding aannemen. Dit betekent dat de *DPO* proactief via interne monitoring controleert of de voorwaarden voor een rechtmatige en veilige verwerking van persoonsgegevens worden nageleefd (zie verder).

3.3. Camerabewaking en de toepassing van de WGB

11. Sinds de aanpassingswet van 21 maart 2018 kan de beslissing om in de openbare ruimtes camera's te plaatsen nog enkel door een openbare overheid worden genomen, zoals de gemeente[19]. Wanneer de politie gebruik maakt van

---

[14] Wet van 21 maart 2018 tot wijziging van de wet op het politieambt om het gebruik van camera's door de politiedienst te regelen, en tot wijziging van de wet van 21 maart 2007 tot regeling en van de plaatsing en het gebruik van bewakingscamera's, de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten en de wet van 2 oktober 2017 tot regeling van de private en bijzondere veiligheid, *BS* 16 april 2018.

[15] Art.4.14 AVG:
"*"Biometrische gegevens": persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijke persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen en vingerafdrukken*". Het gaat met andere woorden om de unieke identificatie of authenticatie van de persoon (overweging 51, AVG).

[16] Zie advies uit eigen beweging "*met betrekking tot het invoeren van camerabewaking door de geïntegreerde politie met het oog op de naleving van de controle van de arbeidsvoorwaarden* (BD20007), te raadplegen op https://www.controleorgaan.be/nl/publicaties/adviezen-aanbevelingen.

[17] Zie voor verdere duiding bij het onderscheid tussen politionele en niet-politionele verwerkingen onder meer, R. SAELENS, 'Europa zet de bakens uit voor de verwerking van persoonsgegevens voor opdrachten van bestuurlijke en gerechtelijke politie: een beknopte verkenning van de Richtlijn politionele en Justitiële verwerkingen', *P&R* 2019, afl. 2, 51-70.

[18] Art. 65 WGB.

[19] Wet van 21 maart 2018 tot wijziging van de wet op het politieambt om het gebruik van camera's door de politiedienst te regelen, en tot wijziging van de wet van 21 maart 2007 tot regeling en van de plaatsing en het gebruik van bewakingscamera's, de wet van 30 november 1998 houdende

camerabewaking zijn de bepalingen van de WPA van toepassing, behalve wanneer het gebruik van camera's in andere wetgeving wordt geregeld[20].

3.3.1. Verwerkingsverantwoordelijke

12. In het gegevensbeschermingsrecht is een belangrijke rol weggelegd voor de 'verwerkingsverantwoordelijke'. Het is "*de natuurlijke persoon of rechtspersoon, de overheidsinstantie, de dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt*"[21]. Wat betreft de verwerkingsactiviteiten in het kader van de opdrachten van bestuurlijke en gerechtelijke politie wordt de verwerkingsverantwoordelijke in de WGB afgebakend tot de "*de bevoegde overheid die, alleen of samen met andere, de doeleinden van en de middelen voor de verwerking van persoonsgegevens vaststelt. Wanneer de doeleinden van en de middelen voor die verwerking door of krachtens een wet, een decreet of een ordonnantie zijn bepaald, is de verwerkingsverantwoordelijke de entiteit die door of krachtens de wet, het decreet of de ordonnantie als de verwerkingsverantwoordelijke wordt aangewezen*".[22] Onder de "*bevoegde overheden*" wordt begrepen "*a) de politiediensten in de zin van artikel 2, 2°, van de wet van 7 december 1998 tot organisatie van een geïntegreerde politie gestructureerd op twee niveaus*"[23].

13. Hoewel de verwerkingsverantwoordelijke in de WPA op bepaalde plaatsen een (specifieke) rol wordt toebedeeld, is dat niet het geval wat betreft het cameragebruik. Zoals hiervoor gezegd is de verwerkingsverantwoordelijke een essentiële actor bij de verwerking van persoonsgegevens. Hij moet namelijk aantonen dat de persoonsgegevens in overeenstemming met het wettelijk kader worden verwerkt. Hij, zijn aangestelde of gemachtigde, is ook de persoon tegenover wie eventuele corrigerende maatregelen kunnen worden opgelegd of strafrechtelijk kan aangesproken worden[24].

De korpschef is de verwerkingsverantwoordelijke voor het bewaren van camerabeelden in een lokale technische gegevensbank[25]. De korpschef is ook de verwerkingsverantwoordelijke voor de bijzondere gegevensbanken[26].

3.3.2. Procedurele vereisten

14. Vooraleer een politiedienst camerabewaking op het grondgebied van een gemeente wenst in te voeren, heeft zij daartoe de principiële toestemming van de gemeenteraad nodig[27]. Er is evenwel geen toestemming vereist voor het gebruik van camera's op besloten plaatsen waarvan de politie zelf de beheerder is, zoals een politiecommissariaat[28]. Het is van belang er op te wijzen dat wanneer de toestemming van de gemeenteraad reeds vóór de wetswijzing van 21 maart 2018 werd verkregen onder de toepassing van de camerawet van 21 maart 2007 de toestemming niet opnieuw van de gemeenteraad verkregen moet worden[29]. Deze initieel bekomen toestemming blijft dus geldig. Dezelfde toestemming kan evenwel niet gebruikt worden voor het gebruik van nieuwe types van camera's die door de wet van 21 maart 2018 werden ingevoerd. Zo legt de WPA specifieke voorwaarden op voor het gebruik van verplaatsbare vaste camera's waarover de gemeenteraad zich moet uitspreken[30]. In dat geval moet dus een nieuwe, of aanvullende, toestemming van de gemeenteraad verkregen worden.

---

regeling van de inlichtingen- en veiligheidsdiensten en de wet van 2 oktober 2017 tot regeling van de private en bijzondere veiligheid, B.S. 16 april 2018.

[20] Zoals trajectcontrole, die onder de toepassing van de wet van 16 maart 1968 betreffende de politie op het wegverkeer valt (Parl. St. Kamer 2017-2018, nr. 54-2855/001, 9).

[21] Art. 4. 7) AVG.

[22] Art. 26, 8° WGB.

[23] Art. 26, 7° WGB.

[24] Zie de artikelen 221 en 222 WGB. Concreet kan het Controleorgaan onder meer de volgende maatregelen nemen (art. 25.2 AVG):
- een waarschuwing geven;
- een berisping geven;
- gelasten om binnen een bepaalde termijn de verwerking in overeenstemming te brengen met het wettelijk kader;
- tijdelijke of definitieve verwerkingsbeperking of verwerkingsverbod opleggen.

[25] Art. 44/11/3sexies § 1, 2de lid WPA.

[26] Artikel 44/4 § 1, 3e lid WPA.

[27] Art. 25/4 § 1, 1° WPA.

[28] Memorie van Toelichting bij deze wet, p. 21 (Parl. St. *Kamer* 2017-2018, nr. 54-2588/001).

[29] Art. 88 wet van 21 maart 2018 en Memorie van Toelichting bij deze wet, p. 113-114 (Parl. St. *Kamer* 2017-2018, nr. 54-2588/001).

[30] Art. 25/4 § 2, 2de lid WPA.

3.3.3. Bewaartermijn van de beelden

15. De camerabeelden kunnen maximaal 1 jaar worden bewaard[31]. De wet bepaalt geen minimumtermijn. Wat de klassieke camerabeelden betreft, bepaalt de WPA niet op welke gegevensdrager de beelden moeten opgeslagen worden. Daarom is het aangewezen dat de korpschef in het register met betrekking tot de verwerking van persoonsgegevens, zoals geregeld in artikel 55 WGB (zie randnummer 3.3.8), aangeeft op welke gegevensdrager de beelden worden opgeslagen. Deze gegevensdrager moet toegankelijk zijn voor het Controleorgaan.

3.3.4. Technische gegevensbanken

16. Voor het gebruik van *ANPR* camera's geldt een specifieke regeling. Het gaat om "*intelligente camera's*", met name "*camera's die ook software bevat die al dan niet gekoppeld wordt aan registers of bestanden, de verzamelde beelden al dan niet autonoom kunnen verwerken*"[32]. Wanneer *ANPR* camerabewaking wordt toegepast, moeten de beelden in een "*technische gegevensbank*" worden opgeslagen,[33] waarbij de persoonsgegevens en informatie tevens worden doorgezonden naar de nationale technische gegevensbank[34]. De beelden kunnen maximum een jaar worden bewaard en ook hier is geen minimumtermijn bepaald[35].

De technische gegevensbank bevat, indien ze verschijnen op de beelden, de volgende gegevens[36]:
1) de datum, het tijdstip en de precieze plaats van langsrijden van de nummerplaat;
2) de kenmerken van het voertuig dat verbonden is aan deze nummerplaat;
3) een foto van de nummerplaat aan de voorkant van het voertuig en in voorkomend geval, aan de achterkant;
4) een foto van het voertuig;
5) in voorkomend geval, een foto van de bestuurder en van de passagiers;
6) de loggingsgegevens van de verwerkingen.

Deze gegevens moeten dus in de technische gegevensbank worden opgenomen voor zover *ANPR* beelden deze gegevens bevatten.

3.3.5. Toegang tot de beelden

17. De toegang tot de beelden is afhankelijk van de finaliteit en gelijk geregeld voor zowel de gewone camerabewaking als voor het gebruik van *ANPR*-camera's. In beide gevallen kunnen de beelden maximum 12 maanden worden bewaard. Wat betreft de opdrachten van bestuurlijke politie is de toegang beperkt tot de eerste maand na de registratie van de beelden. Voor opdrachten van gerechtelijke politie zijn de beelden over de volledige bewaartermijn toegankelijk, waarbij na de eerste maand de tussenkomst van de procureur des Konings is vereist[37]. De toegang moet gemotiveerd en operationeel noodzakelijk zijn voor het uitvoeren van een specifieke opdracht[38]. Dit komt er op neer dat de toegang tot de beelden alleen toegelaten is voor personen die deze persoonsgegevens en informatie nodig hebben en wanneer daartoe dus een concreet operationeel belang aanwezig is[39].

3.3.6. Zichtbaar en niet-zichtbaar gebruik van camera's

18. Zichtbare camera's zijn camera's waarbij het gebruik ervan wordt aangekondigd door pictogrammen, de camera's gemonteerd zijn in als zodanig herkenbare politievoertuigen, -vaartuigen, -luchtvaartuigen of elk ander vervoermiddel van de politie of gedragen worden door politieambtenaren die als zodanig herkenbaar zijn[40]. In uitzonderlijke situaties kan de politie heimelijk gebruik maken van camera's (niet-zichtbaar gebruik van camera's). Daarbij kan de camera gedragen worden door de politieambtenaar of in een anoniem politievoertuig geplaatst zijn. Er is sprake van een anoniem politievoertuig wanneer het politievoertuig niet als zodanig herkenbaar is. In dat geval is er dus sprake van

[31] Art. 25/6, 44/11/3decies § 2, eerste lid, en 46/12, eerste lid WPA.
[32] Art. 25/2 § 1, 3°, juncto 44/2 § 3, derde lid WPA.
[33] Art. 44/2 § 3, eerste lid, WPA.
[34] Art. 44/11/3sexies WPA.
[35] Art. 44/11/3decies § 2, eerste lid WPA.
[36] Art. 44/11/3decies § 1 WPA.
[37] Art. 25/7 § 1, 1ste en 2de lid en 44/11/3decies § 3, tweede lid WPA.
[38] Art. 44/11/3decies § 3, 1ste lid WPA.
[39] Memorie van Toelichting bij deze wet, p. 29 (Parl. St. *Kamer* 2017-2018, nr. 54-2588/001).
[40] Art. 25/2 § 2 WPA.

"niet-zichtbaar" cameragebruik[41]. De toepassing van niet-zichtbare camera's is strikt geregeld en beperkt tot vier situaties. Met name:
1) omwille van bijzondere omstandigheden, met name bij grote volkstoelopen met het oog op het inwinnen van informatie van bestuurlijke politie over geradicaliseerde personen of *terrorist fighters* en op anonieme politievoertuigen voor het automatisch inlezen van nummerplaten, teneinde geseinde voertuigen op te sporen (art. 46/4 WPA);
2) bij de voorbereiding van acties van gerechtelijke politie of bij de handhaving van de openbare orde tijdens deze acties (artikelen 46/7, 46/8 WPA);
3) in het kader van de gespecialiseerde opdrachten van bescherming van personen (art. 44/9 WPA) en
4) tijdens de overbrenging van aangehouden of opgesloten personen (art. 46/11 WPA).

Behalve wanneer het niet-zichtbaar gebruik van camera's onder het gezag van een magistraat wordt uitgevoerd, moet deze vorm cameragebruik evenwel voorafgaand aan het Controleorgaan worden aangeven. Deze voorafgaande mededeling moet het Controleorgaan toelaten om de wettelijkheid van de beslissing te beoordelen[42].

3.3.7. Impact- en risicoanalyse en gegevensbeschermingseffectbeoordeling (GEB of *DPIA, Data Protection Impact Assessment*)

19. Sedert de wet van 21 maart 2018 is het verplicht om, voorafgaand aan het gebruik van camerabewaking, een impact- en risicoanalyse op te maken waarbij de bescherming van de persoonlijke levenssfeer wordt afgetoetst aan en tegenover het operationele niveau van het cameragebruik[43]. Deze oefening moet ook worden gemaakt vóór het oprichten van een (lokale) technische gegevensbank[44]. Hiervoor wordt de bijstand van de *DPO* gevraagd[45].

Mits de voorwaarden van de WGB voor een *DPIA* en de voorwaarden voor een risico- en impactanalyse betreffende het zichtbaar gebruik van camera's en/of betreffende de oprichting van technische gegevensbanken onder de WPA voldaan zijn, kunnen beide analyses in één document vervat zijn. Aangezien een DPIA onder de WGB een bredere analyse vergt dan hetgeen in de WPA is voorgeschreven, wordt er op gewezen dat, ingeval beiden samen worden behandeld, die analyse conform de WGB alle relevante systemen en procedures van verwerkingsactiviteiten moet bestrijken. Behalve de naleving van de WGB en de WPA moeten tevens de operationele voorzorgsmaatregelen en beveiligingsmaatregelen worden omschreven (die worden genomen om de risico's voor de te beschermen persoonsgegevens te beperken).

3.3.8. Register

20. Het gebruik van camerabewaking moet in een (lokaal) register worden bijgehouden[46]. In het register wordt het type camera's en de locatie opgenomen. Er is evenwel nog geen Koninklijk besluit uitgevaardigd waarbij de inhoud van het register nader wordt uitgewerkt. Niettemin is het Controleorgaan van oordeel dat in het licht van de effectiviteit van haar toezichtsbevoegdheden de politiedienst, in afwachting van het uitvoeringsbesluit, uit eigen beweging een register aanlegt waarop elk gebruik van (type) camera's wordt vermeld, inbegrepen het niet-zichtbaar gebruik van camera's. Op die manier verkrijgt het Controleorgaan (en trouwens de politiezone zelf ook en wel in de eerste plaats) (in)zicht (op) over het gebruik van camerabewaking op het grondgebied van de gemeente dat onder de bevoegdheid van de politiedienst valt. Tegelijk kan het gebruik van camerabewaking afgetoetst worden aan het register van de verwerkingsactiviteiten (zie verder). Aangezien er door het filmen persoonsgegevens worden verwerkt, moet deze verwerking ook in het register van verwerkingen opgenomen worden[47]. Beide registers zijn of moeten beschikbaar zijn voor het Controleorgaan.

3.3.9. Logging

21. De politie is verplicht om logbestanden bij te houden[48]. Een logbestand is bij uitstek een instrument om het bewijs van de (on)rechtmatigheid van de verwerking te controleren en de integriteit en de beveiliging van de gegevens te

[41] Art. 46/4 e.v. WPA.
[42] Art. 46/6 en 46/10 WPA.
[43] Art. 25/4 § 2 WPA.
[44] Art. 44/11/3octies WPA.
[45] Art. 65, 3° juncto 58 WGB.
[46] Art. 25/8 WPA.
[47] Art. 55 WGB.
[48] Art. 56 § 1 WGB, ter uitvoering van artikel 25 Richtlijn Politie & Justitie en art. 44/11/3decies § 1, 6° WPA.

garanderen[49]. In dat verband zijn logbestanden tevens van belang bij interne tuchtprocedures of administratieve onderzoeken. Logbestanden zijn bijgevolg van belang met het oog op zowel proactieve als reactieve controle en zowel op intern als op extern niveau.

22. logbestanden moeten worden onderscheiden van de *login* of de toegang tot het verwerkingssysteem om de gegevens te kunnen raadplegen. Wat de toegang tot de camerabeelden betreft (van de stadscamera's en het politiegebouw), bevat de WPA geen specifieke regeling met betrekking tot de profielen die toegang hebben tot de camerabeelden. Als algemene regel geldt dat de toegang tot de beelden beveiligd is en de concrete reden van toegang wordt geregistreerd[50]. Niettemin gelden in dat verband de algemene regels van de WGB en de specifieke bepalingen van de WPA. Dit betekent dat de toegang tot de beelden alleen toegelaten is voor personen die de persoonsgegevens en informatie nodig hebben wanneer daartoe een concreet operationeel belang aanwezig is en de toegang traceerbaar is[51].

3.4. functioneel beheer

23. De politionele en gerechtelijke gegevens zijn bijzonder gevoelig. Zij mogen enkel in het kader van opdrachten van gerechtelijke of bestuurlijke politie worden verwerkt, in overeenstemming met de wettelijke voorschriften (WPA,WGB, MFO 3[52], het wetboek van strafvordering, het beroepsgeheim, het geheim van het onderzoek, enz. …). Daarom wordt ieder gebruik van de toepassingen die aan de ANG verbonden zijn (registratie of wijziging van een gegeven, de raadpleging, enz. …) gekoppeld aan toegangsprofielen en de toegang tot de gegevens in een logbestand bijgehouden. Hetzelfde geldt voor ieder gebruik van het Rijksregister of de gegevens van de DIV[53]. Ook uitgevoerde verwerkingen in de basisgegevensbanken maken het voorwerp uit van logbestanden die bewaard worden gedurende vijftien jaar vanaf de in de basisgegevensbanken uitgevoerde verwerking. De verwerkingsverantwoordelijke kan, indien nodig, deze termijn verlengen met een maximale periode van vijftien jaar[54].

De ministeriële richtlijn MFO 6[55]regelt de acht basisfunctionaliteiten[56]van de AIK werking. In het raam van de organisatie en in plaats stelling van de informatiestromen, moet het AIK een belangrijke ondersteunende rol spelen ten voordele van de functionele beheerders in de politiezones. Deze ondersteuning uit zich op het niveau van de begeleiding, de kwaliteitscontrole en de opvolging van de opgemerkte of gesignaleerde problemen.

4. ONDERZOEKSBEVINDINGEN EN JURIDISCHE ANALYSE

4.1. Politionele verwerkingen

4.1.1. Het gebruik van klassieke camerabewaking en ANPR-camera's: goedkeuring gemeenteraad

24. De PZ beschikt over een aantal vaste camera's met het oog op het toezicht op een beperkt aantal publieke plaatsen (openbare ruimte), in het politiecommissariaat, 3 vaste *ANPR* camera's bij de grensovergang België – Nederland, en

[49] Art. 56 § 2 WGB.
[50] Art. 25/7 § 1, 3e lid, 44/4 § 2, 2de en 3de lid 44/11/3*novies* WPA. Deze laatsten verplichten het bijhouden van logbestanden voor de verwerking van persoonsgegeven en informatie in de operationele (technische) gegevensbanken.
[51] Zie supra en de memorie van Toelichting bij de wet van 21 maart 2018, p. 29 en 30 (Parl. St. *Kamer* 2017-2018, nr. 54-2588/001).
[52] De gemeenschappelijke richtlijn MFO 3 van de Ministers van Justitie en van Binnenlandse Zaken "*betreffende het informatiebeheer inzake gerechtelijke en bestuurlijke politie*".
[53] Dienst Inschrijving Voertuigen.
[54] Art 44/11/2 §8 WPA.
[55] Gemeenschappelijke en dwingende richtlijn MFO 6 van de ministers van Justitie en Binnenlandse zaken van 9 januari 2003 "*betreffende de werking en organisatie van de arrondissementele informatiekruispunten"* (AIK).
[56] Deze acht basisfunctionaliteiten zijn:
1. Opvolging van gebeurtenissen en feiten die zich recent hebben voorgedaan om snel de bovenlokale veiligheidsproblemen te detecteren en te identificeren
2. Identificatie van verbanden tussen gebeurtenissen of feiten en antecedenten
3. Ondersteuning van de coördinatie en de opvolging van aangemelde onderzoeken
4. Opvolging van gebeurtenissen en feiten in tijd en ruimte
5. Steun in het raam van de geïntegreerde fenomeenopvolging
6. Ondersteuning van de opvolging van dader- en slachtoffergroepen
7. Bijdrage tot de grensoverschrijdende uitwisseling van politionele informatie
8. Ondersteuning van de functionele beheerders van de informatieverwerking binnen de politiezones

omgekeerd en 1 mobiele *ANPR* camera. Uit de vaststellingen blijkt dat de vaste *ANPR* camera's door 2 besluiten van de gemeenteraad werden goedgekeurd:

- Gemeenteraad van 19 december 2017;
- Gemeenteraad van 22 mei 2018;

25. De goedkeuring van de gemeenteraad op de zitting van 19 december 2017 heeft betrekking op 1 *ANPR* camera ter hoogte van de grensovergang[57]. De goedkeuring van de gemeenteraad op de zitting van 22 mei 2018 heeft betrekking op de overname van 2 *ANPR*-camera's van de federale politie aan een andere grensovergang .

26. Er werd aan het Controleorgaan daarentegen geen goedkeuring van de gemeenteraad voorgelegd voor het plaatsen en gebruik van vaste camera's die exclusief door de politie worden gebruikt om toezicht te houden op de publieke plaatsen. De PZ heeft daarnaast 1 zichtbare mobiele *ANPR*-camera, gemonteerd in een als zodanig herkenbaar politievoertuig. Deze wordt gebruikt voor het automatisch inlezen van nummerplaten van voertuigen die geseind worden. Ook voor deze mobiele *ANPR*-camera beschikte de PZ niet over een goedkeuring van de gemeenteraad. **Daardoor was het gebruik van vaste camera's met het op het houden van toezicht op de publieke ruimte en het gebruik van de mobiele *ANPR* camera niet in overeenstemming met artikel 25/4 § 1, 1° WPA.**

In antwoord op het ontwerprapport wordt gesteld dat de PZ op 24 november 2020 de toestemming van de gemeenteraad heeft verkregen voor het gebruik van deze camera's. Het Controleorgaan neemt kennis van het gemeenteraadsbesluit en schrapt in dat opzicht de voorgenomen corrigerende maatregel van het ontwerprapport (in het ontwerp aangeduid als maatregel "a") m.b.t. de vaste camera's met het oog op het houden van toezicht op de publieke ruimte en de mobiele *ANPR* camera.

4.1.2. Verwerkingsverantwoordelijke voor de vaste *ANPR*-camera's

27. Er werd tijdens het plaatsbezoek vastgesteld dat de politie van er van uitgaat de twee vaste *ANPR*-camera's aan de grensovergang met Nederland niet onder de verantwoordelijkheid van de PZ vallen. De PZ verwijst daarvoor naar het in randnummer 24 vermeld goedkeuringsbesluit van 22 mei 2018.

28. Uit het besluit blijkt dat de politiezone beide vaste *ANPR* camera's van de federale politie overneemt. De beelden van de ANPR camera's worden niet op de server van de PZ bewaard maar wel op de centrale backoffice van de federale politie Limburg (CSD/SICAD)[58]. Doordat de PZ de beelden niet bewaart en ook geen directe toegang tot de bewaarde beelden heeft, wordt door de PZ aangenomen dat zij niet als verwerkingsverantwoordelijke kan worden beschouwd.

29. Het Controleorgaan kan de visie van de PZ niet bijtreden. Uit het gemeenteraadsbesluit blijkt dat de 2 vaste *ANPR* camera's aan de PZ werden overgedragen waardoor zij op dat ogenblik als verwerkingsverantwoordelijk dient aangemerkt te worden. De federale politie heeft immers vanaf dat moment geen zeggenschap meer over deze vaste *ANPR* camera's (de federale politie bepaalt niet (meer) het doel en de middelen). De beslissing om al dan niet de *ANPR* camera's te gebruiken ligt immers volledig in handen van de PZ. Dat de PZ zelf geen toegang heeft tot de camerabeelden is geen noodzakelijke voorwaarde om als verwerkingsverantwoordelijk aangeduid te worden. In het kader van de WPA wordt immers niet vereist dat de lokale politiezone zelf de beelden bewaart. De PZ *kan* een lokale technische gegevensbank oprichten (waarin de beelden en samenhangende gegevens worden bewaard), maar moet dan niet doen. In ieder geval moeten de beelden rechtstreeks worden doorgestuurd naar de nationale technische gegevensbank[59]. Voor het bewaren van de beelden (en de samenhangende gegevens) in de nationale technische gegevensbank zijn daarentegen wél de ministers van Binnenlandse Zaken en Justitie als verwerkingsverantwoordelijke aangeduid[60] ook al gaat het om *ANPR* camera's die door de lokale politie worden geplaatst en gebruikt.

30. Dat de beelden voorlopig (nog) op de arrondissementele backoffice worden bewaard, doet dus niets af aan de vaststelling dat de PZ als verwerkingsverantwoordelijke moet beschouwd worden voor de *ANPR* camera's aan de grensovergang met Nederland. Bijgevolg geldt dat ook voor de *ANPR* camera aan de

[57] Merk op dat vanuit juridisch oogpunt strikt genomen de 'gunning' van de aankoop van camera's op zichzelf niet tevens de 'goedkeuring' tot het plaatsen en gebruiken' van de camera's, zoals bedoeld in artikel 25/4 § 1, 1° WPA, impliceert.
[58] Zie rubriek 3.3.1.
[59] Art. 44/11/3sexies § 2 WPA
[60] Art. 44/11/3sexies § 1 WPA.

grensovergang, die door het in randnummer 24 vermeld besluit van de gemeenteraad van 19 december 2017 werd goedgekeurd, ondanks dat blijkens het besluit de "*HITS op de genoemde blacklist (…) via de Centrale Back Office worden doorgestuurd naar het bevoegde CIC (…)*".

4.1.3. Bewaartermijn van de beelden en technische gegevensbank

31. De gewone beelden van de vaste camera's (politiecellen, het politiegebouw en publieke ruimte) worden op een lokale server van de politie bewaard tot een gemiddelde van maximum 26 dagen. Deze korte bewaartermijn is te wijten aan een beperkte opslagcapaciteit waardoor de beelden na deze termijn worden overschreven door nieuwe beelden[61].

32. De beelden van de mobiele *ANPR* camera worden niet op een afzonderlijke server bewaard. Er worden hits gegenereerd maar deze worden niet doorgestuurd naar een andere (nationale) technische gegevensbank. Gelet op het feit dat de correlatie plaatsvindt op een applicatie op de laptop in het voertuig en dat deze applicatie de lijsten verwerkt die nodig zijn om de correlatie te laten plaatsvinden, dient echter de laptop beschouwd te worden als een lokale technische gegevensbank voor de mobiele *ANPR* beelden. **Aldus beschikt de PZ over een lokale technische gegevensbank voor de mobiele *ANPR*-beelden (zie verder 4.1.7).**

4.1.4. Politiecellen

33. Het Controleorgaan kon vaststellen dat in de politiecellen in het politiegebouw van de PZ camerabewaking wordt toegepast in overeenstemming met artikel 10 van het Koninklijk besluit van 14 september 2007[62].

4.1.5. Andere types van camerabewaking

34. Volgens de PZ worden geen andere vormen van camerabewaking toepast, zoals het gebruik van *bodycams* of niet zichtbaar gebruik van camera's. Geconfronteerd met informatie van een persbericht van 2016 waarbij door de PZ het (niet-zichtbaar) gebruik van mobiele en verplaatsbare vaste camera's werd aangekondigd met het oog op de bestrijding van overlast en sluikstorten werd aan het COC medegedeeld dat dit éénmaal heeft plaatsgevonden. Het werd stopgezet omdat bleek dat het gebruik van de camera's niet in overeenstemming was met de vigerende wetgeving. Het Controleorgaan neemt hiervan akte.

4.1.6. Toegang tot de beelden (login) en logging (tijdstip, reden van bevraging)

35. Bij de PZ is de toegang tot de camerabeelden niet afhankelijk van het type van cameragebruik. De beelden van de stadscamera's, het cellencomplex en de bewaking van het politiegebouw zijn toegankelijk voor het operationeel personeel op basis van een algemene dienstlogin en een paswoord.

Het gebruik van een algemene dienstlogin is niet in overeenstemming met de wettelijke verplichtingen. Dit betekent dat er geen gebruik wordt gemaakt van een individualiseerbare toegang tot de camerabeelden. Daarnaast wordt er geen logbestand van de toegang tot de beelden bijgehouden. Het Controleorgaan stelde bijgevolg vast dat de toegang tot de camerabeelden niet kan gecontroleerd worden waardoor geen controle op de (on)rechtmatigheid van de toegang tot de camerabeelden kan uitgevoerd worden, wat nochtans een wettelijk verplichting is[63].

36. De PZ beschikte niet over een adequaat uitgewerkt toegangs- en gebruikersbeheer tot de camerabeelden. Dat dit problematisch is, wordt duidelijk aan de hand van de hiervoor vastgestelde tekortkoming inzake de toegang tot de camerabeelden.

Corrigerende maatregel

[61] Door het "*overschrijven*" van de beelden, worden de plaats van de beelden ingenomen door de nieuwe beelden.
[62] KB van 14 september 2007 betreffende de minimumnormen, de inplanting en de aanwending van de door de politiediensten gebruikte opsluitingsplaatsen, *BS* 16 oktober 2007.
[63] Art. 25/7 § 1, 3de lid WPA en 56 WGB. Voor de volledigheid wordt opgemerkt dat de politie van zich niet kan beroepen op artikel 284 WGB. Op grond van deze bepaling moeten de geautomatiseerde verwerkingssystemen die vóór 6 mei 2018 door de – in casu – PZ werden opgezet pas tegen uiterlijk 6 mei 2023 in overeenstemming worden gebracht met artikel 56, § 1 WGB (loggings). Aangezien het cameranetwerk door de politiezone ook na 6 mei 2018, en in ieder geval wat betreft de ANPR camera's slechts in 2017, plaats vond, is deze uitzondering niet van toepassing.

De toegang tot de camerabeelden moet in overeenstemming met artikel 25/7, § 1, 3e lid, WPA, worden gebracht zodat de reden van de bevragingen geregistreerd wordt. Het bewijs van deze wetsconforme implementatie wordt binnen de negen maanden na datum van kennisname van deze corrigerende maatregel aan het Controleorgaan overlegd.

Corrigerende maatregel
De logbestanden moeten overeenkomstig artikel 56 WGB worden bijgehouden. Het bewijs van deze wetsconforme implementatie wordt binnen de negen maanden na datum van kennisname van deze corrigerende maatregel aan het Controleorgaan overlegd.

4.1.7. Impact- en risicoanalyse en gegevensbeschermingseffectbeoordeling (GEB of *DPIA, Data Protection Impact Assessment*)

37. De PZ heeft een *DPIA* voor (de verschillende vormen van) cameragebruik in de politiezone voorgelegd. Het COC merkt evenwel op dat wat betreft de lokale *ANPR* camera's niet kan teruggevallen worden op de *DPIA* van de nationale technische gegevensbank (AMS[64]). De *DPIA* van AMS heeft geen betrekking op camera's (van de lokale politiezones) als zodanig. Het COC stelde vast dat **voorafgaand aan de oprichting van de lokale technische gegevensbank (zie 4.1.3) geen *DPIA* werd gemaakt, terwijl dat een wettelijke verplichting is[65].** De *DPIA* dateert immers van 27 oktober 2020 terwijl de PZ reeds een geruime tijd voorafgaand aan de visitatie gebruik maakte van een mobiele *ANPR* camera.

De door de PZ opgemaakte *DPIA's* voor het gebruik van de camera's werden aan een *prima facie* analyse[66] onderworpen. Het Controleorgaan heeft drie algemene opmerkingen. Ten eerste kan het personeel van de geïntegreerde politie niet als een 'verwerker' worden beschouwd. Het gaat ter zake om aangestelden die over toegangsrechten beschikken om hun opdrachten te kunnen uitvoeren. Dat is anders wat betreft externe dienstverleners (leveranciers) die toegang tot de gegevens hebben in het kader van hun contractuele afspraken. Ten tweede heeft de burger geen recht van 'bezwaar' voor werkingen die door de wet (WPA) worden geregeld[67]. Tot slot kan de overgangsbepaling van artikel 284 WGB[68] niet ingeroepen worden voor gegevensbanken (zoals een technische gegevensbank) die na de omzetting van de *LED* in de WPA worden geregeld[69]. Het Controleorgaan herhaalt ten overvloede dat artikel 56 betrekking heeft op logbestanden en niet op de toegangsrechten tot de gegevens.

Wat betreft de *DPIA* met betrekking tot het gebruik van de mobiele *ANPR* camera wordt in de *DPIA* ten onrechte aangenomen dat er geen beelden van de nummerplaat worden gemaakt. Er is ontegensprekelijk een technische verwerking (opslag) van de foto van de nummerplaat nodig om de nummerplaat te kunnen lezen en met de *blacklists* te correleren. Ten tweede is alleen een advies van de DPO verplicht wanneer gebruik wordt gemaakt van beoordelingscriteria en dus niet voor de aangeleverde *blacklist*. **Het Controleorgaan beschouwt de betrokkenheid van de DPO bij het gebruik van lokale lijsten wel als een *best practice*.**

4.1.8 Register van camerabeelden en verwerkingsactiviteiten

38. De politie van heeft geen (afzonderlijk) register van cameragebruik aangelegd. Het cameragebruik is daarentegen wel als finaliteit opgenomen in het lokaal register van verwerkingen. Zoals hiervoor wordt toegelicht, is de inhoud van het lokale cameraregister nog niet door een uitvoeringsbesluit geregeld. Dit mag de korpschef er niet van weerhouden om op eigen initiatief een (voorlopig) lokaal register van cameragebruik aan te leggen. Om praktische redenen kan het COC ermee instemmen dat het cameragebruik voorlopig in een specifiek onderdeel van het een register van de verwerkingen wordt opgenomen. Het is daarbij aangewezen dat ook de types van camera's (vast, mobiel, ANPR, zichtbaar of niet zichtbaar gebruik) in dit onderdeel van het verwerkingsregister worden vermeld**.**

[64] *ANPR Managed Services*.
[65] Art. 44/11/3octies WPA.
[66] Een *prima facie* analyse houdt een marginale toets in en betekent geen formeel advies in de zin van art 59 GBW.
[67] Dit recht komt niet voor in titel 2 WGP (politionele verwerkingen). Daarnaast bepaalt artikel 21 AVG, voor zover van belang, dat het recht van bezwaar alleen geldt voor verwerkingen in het kader van artikel 6, 1ste lid, e) of f, met name wanneer de verwerking niet gebaseerd is op een wettelijke regeling maar voor de uitvoering van een taak van algemeen belang of wanneer de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of een derde zwaarder wegen dan de rechten van de betrokkene.
[68] Volgens artikel 284 WGB moeten de systemen voor geautomatiseerde verwerking die vóór 6 mei 2016 door de politiediensten werden opgezet, uiterlijk op 6 mei 2023 in overeenstemming gebracht met artikel 56 § 1 WGB.
[69] Zie de artikelen 44/4 § 2 en 44/11/3novies WPA.

Verzoekt,
dat de korpschef, in afwachting van het uitvoeringsbesluit inzake het lokaal cameraregister, een lokaal register van het cameragebruik aanlegt of in een afzonderlijk luik in het register van verwerkingen opneemt waarin de types van camera's en de doeleinden en het opslagmedium van de beelden duidelijk worden vermeld.

4.1.9. De koppeling van ANPR-beelden met lokale lijsten

39. De ANPR-beelden van de vaste en de mobiele ANPR-camera's worden gekoppeld aan bepaalde objectieve lijsten. Het betreffen de zogenaamde 'Optie 32'[70], of '*blacklists*', en de 'Bodoc-lijst'. Deze laatste betreft een lijst met internationale nummerplaten die betrekking heeft op onbetaalde verkeersboetes.

40. Voor de correlaties wordt gebruik gemaakt van nationale lijsten en lokale lijsten. Op het vlak van het verkrijgen van de nationale lijsten is het niet de PZ zelf maar een andere PZ die de daarvoor noodzakelijk optie 32[71]uitvoert. Het gebruik van de optie 32 door de PZ wordt aldus niet rechtstreeks gelogd. Dit kan problematisch zijn in het licht van de gegevensbescherming omdat men aldus niet exact weet welke politiedienst of politie-entiteit de gedownloade gegevens van de unieke bronnen die aan de basis liggen van de correlaties, gebruikt. Blijkens de *DPIA* van de mobiele *ANPR* camera worden de *blacklists* geëncrypteerd doorgestuurd via email naar de PZ die deze vervolgens via een USB-stick op de laptop van de mobiele ANPR importeert. De laptop is een *stand alone* die niet met het internet is verbonden[72]. Van deze verkregen lijsten worden enkel de nummerplaten weerhouden, alsmede de titel van de lijst. Er wordt dus geen gebruik gemaakt van de (samenhangende) aangeleverde metadata. Het Controleorgaan wijst er op dat deze gegevens (landcode, reden(en) van de seining, de te nemen maatregel(en) en de voor deze maatregelen verantwoordelijke politiedienst of land) noodzakelijk zijn omdat zij mee invulling geven aan het minimale, nationale actiebeleid (operationele Fiche C02).

41. Deze nationale lijsten worden aangevuld met lokale lijsten van de PZ. De input voor deze lokale lijsten is afkomstig van de dienst interventie en van de lokale recherchedienst, **maar de criteria voor opname op deze lokale lijsten konden niet verduidelijkt worden.**

Corrigerende maatregel
De criteria voor opname op deze lokale lijsten dienen verduidelijkt te worden aan de hand van de richtlijn inzake koppelingen en correlaties enerzijds, en de fiche C02 (van het boek 1 van de MFO 3)[73] *anderzijds, en binnen de drie maanden na kennisname van deze corrigerende maatregel aan het Controleorgaan worden overgemaakt.*

[70] Optie 32 verstrekt toegang tot:
- een bestand met gestolen Belgische voertuigen en nummerplaten (ANG);
- een bestand van deze voertuigen met de datum van de feiten (ANG);
- een bestand met voertuigen uit de ANG met een binding met een persoon die voorkomt in de ANG (met uitzondering van deze die onderworpen zijn aan een beperkte of bijzondere toegang);
- een bestand met voertuigen ingeschreven bij DIV (Directie Inschrijvingen Voertuigen van de FOD Mobiliteit en Vervoer) op naam van een in de ANG gekende persoon (met uitzondering van deze die onderworpen zijn aan een beperkte of bijzondere toegang);
- een bestand met vermoedelijk niet-verzekerde Belgische voertuigen (Veridass);
- een bestand met vermoedelijk niet-verzekerde Belgische voertuigen per eenheid (Veridass);
- een bestand met niet-gekeurde Belgische voertuigen (GOCA)
- een bestand met niet-gekeurde Belgische voertuigen per eenheid (GOCA);
- een bestand met gestolen Nederlandse voertuigen (Nederlandse politie);
- een bestand met in SIS II geseinde voertuigen.

[71] De optie 32 is politiejargon voor het uitvoeren van een *download* van specifieke ANG gegevens naar de politiezone die deze vraagt. De uitvoering van deze optie wordt gelogd, waardoor het mogelijk is om deze per eenheid op te volgen. De optie 32 wordt hoofdzakelijk gebruikt voor de download van de gegevens afkomstig van ANG (nationaal te nemen maatregelen ten aanzien van voertuigen en nummerplaten), SIS (internationaal te nemen maatregelen ten aanzien van voertuigen, niet ouder dan twee jaar), GOCA (vermoedelijk niet gekeurde voertuigen) en VERIDASS (vermoedelijk niet verzekerde voertuigen). Deze gegevens kunnen worden gebruikt voor correlatie in de technische gegevensbanken met het oog op het uitvoeren van het door de werkgroep politie-justitie-binnenlandse zaken bepaalde actiebeleid, dat op arrondissementeel niveau dient vertaald te worden in een interventiebeleid. De optie 32 bevat tevens gegevens afkomstig vanuit de ANG en DIV waarmee de gegevens inzake de door de ANPR gecapteerde nummerplaten kunnen verrijkt worden. Voor de ANG gaat het om de verrijking met het gegeven of het voertuig of de nummerplaat een binding heeft met een in de ANG gekende persoon; voor de DIV gaat het om het gegeven of de titularis van het voertuig gekend is in de ANG.

[72] *DPIA* mobiele *ANPR* camera, p. 5.

[73] Zie in dat verband de op 28 januari 2021 in het Belgisch staatsblad gepubliceerde Gemeenschappelijke bindende richtlijn van de Ministers van Justitie en van Binnenlandse Zaken "*met betrekking tot de bepaling van de nadere regels voor de toereikende, ter zake dienende en niet overmatige maatregelen met betrekking tot de koppeling of correlatie van de technische gegevensbanken ingevolge het gebruik van intelligente camera's en systemen voor de automatische nummerplaatherkenning, bedoeld in artikel 44/2 § 3 van de wet op het Politieambt, met de gegevensbanken bedoeld*

42. Het uitvoeren van de correlaties gebeurt op een laptop in het politievoertuig. **Deze laptop dient bijgevolg aanzien te worden als een lokale technische gegevensbank in de zin van artikel 44/11/3sexies WPA**[74]**.** Zoals hiervoor vastgesteld, was er ook geen impact- en risicoanalyse beschikbaar voor deze lokale technische gegevensbank. Volgens de PZ worden alleen de laatste *hit* bewaard en overschreven wanneer een volgende *hit* wordt aangemaakt.

In antwoord op het ontwerprapport stelt de PZ zich vragen bij het oordeel dat de laptop voor de mobiele *ANPR* camera als een technische gegevensbank wordt beschouwd. In de eerste plaats verwijst het Controleorgaan naar artikel 44/11/3*decies* WPA waarin wordt bepaald dat de technische gegevensbank wordt gebruikt om persoonsgegevens (nummerplaten) te correleren met *blacklists* of met vooraf bepaalde beoordelingscriteria[75]. In de tweede plaats blijkt de aan het Controleorgaan voorgelegde *DPIA* betrekking te hebben op zowel het cameragebruik als de verwerkingen in de gegevensbank, met name de laptop. Hiervoor wordt in de *DPIA* bovendien melding gemaakt van de artikelen 44/11/3*sexies* tem 44/11/3*decies* WPA; deze hebben betrekking op de technische gegevensbanken.

43. Het realiseren van een *hit* staat in verband met het actie[76]- en het interventiebeleid[77]. Het COC stelde in dat verband vast dat de politiezone niet beschikt over een mobiele connectie met ANG toepassingen zoals de ANG controle. *Hits* worden dan ook radiofonisch afgetoetst via het CIC voor een check van de ANG Controle alvorens te interveniëren. Deze toets kan enkel plaatsvinden voor de lijsten optie 32, doch niet voor de lokale lijsten. Daarom is het actie- en interventiebeleid op lokale lijsten onduidelijk, mede door het ontbreken van de noodzakelijke metadata.

Aanbeveling
Met het oog op een effectieve en efficiënte toepassing van de ANPR verwerkingen is het van belang dat de PZ een duidelijk interventiebeleid voor de hits op nationale lijsten en een duidelijk actie- en interventiebeleid op de lokale lijsten uitwerkt.

44. In het licht van de samenlezing met de overige bepalingen van de WPA en de WGB is het Controleorgaan van oordeel dat de samengestelde lijsten op geregelde tijdstippen geëvalueerd moeten worden. Hieruit volgt dat de lokale lijst niet voor een 'onbepaalde termijn' kan bewaard worden. Er dient voorkomen te worden dat een parallel circuit van politiegegevensbanken ontstaat waarvan de gegevens niet in de door de WPA vastgelegde gegevensbanken kunnen of zullen verwerkt worden.

4.2. De gegevensverwerking in de ANG

4.2.1. Het functioneel beheer

45. Op het vlak van functioneel beheer werkt de PZ samen met 2 andere politiezones (provincie Limburg). Daartoe werkt een beperkte pool van vaste functioneel beheerders samen met een aantal assistent functioneel beheerders in de genoemde politiezones. De functioneel beheerders hebben de mogelijkheid om vanop afstand in te loggen op elkaars werkomgeving. Dit is bevorderlijk voor de snelheid van tussenkomsten en vermindert het aantal verplaatsingen.

Er blijkt sinds 4 jaar opnieuw een goede samenwerking te zijn met het SICAD-AIK op het vlak van de achtste basisfunctionaliteit van de MFO6, met name ondersteuning van de functionele beheerders van de informatieverwerking

in artikel 44/2 §§ 1 en 2 WPA, of met andere gegevensbanken waartoe de politiediensten toegang hebben door of krachtens de wet of internationale verdragen die België binden".

[74] Deze lokale technische gegevensbank stuurt echter geen gegevens door naar de nationale technische gegevensbank. De integratie van de camera (rechtstreekse integratie) of van de LTGB (integratie via een tussenliggende LTGB) dient aangevraagd te worden bij het nationaal ANPR project FedPol DRI BIOPS via het raamcontract R3 043 Proximus/Trafiroad.

[75] Technisch is het bovendien zo, dat de correlatie op zich op geen andere wijze kan verlopen dan via een technische gegevensbank daar de gegevens afkomstig van de unieke bronnen die aan de basis liggen van de correlatie in die technische gegevensbank verwerkt worden.

[76] Het begrip 'Actiebeleid' verwijst naar een combinatie van de 'Reden van Seining' (RvS) en de 'Te Nemen Maatregel' (TNM). De Reden van Seining is dan weer een combinatie van het aard feit, en het criterium op basis waarvan de entiteit aan het feit werd gekoppeld (basisregistratiecriterium). (Vb. RvS: gestolen – zware diefstal, TNM: in beslag nemen). Voor elk van alle theoretisch mogelijke combinaties RvS-TNM werd door een nationale werkgroep politie en justitie een nationaal 'minimaal actiebeleid' vastgesteld, dat moet ondernomen worden indien een bepaalde combinatie voorkomt.

[77] Het interventiebeleid bepaalt hoe, of, door wie en wanneer er politioneel wordt tussengekomen, en zowel in functie van lokaal gemaakte afspraken als van de mogelijkheden tot interventie op het moment zelf.

binnen de politiezones, onder andere door het houden van driemaandelijkse werkvergaderingen met alle functioneel beheerders van het arrondissement. De PZ neemt hier actief aan deel.

46. Het COC stelde een goede werking vast van de fluxen gericht op het voeden van de ANG. Voorafgaand aan de flux naar de ANG vindt er een kwaliteitscontrole plaats van de gegevens. Dit gebeurt casuïstisch en niet aan de hand van structurele 'kwaliteitscontrole parameters' in ISLP. De optie 35[78]wordt op dagelijkse basis uitgevoerd, en bij de verwerpingen en de daaruit voortvloeiende rechtzettingen stellen we nauwelijks achterstand vast. Tot slot maakt de functioneel beheerder geen gebruik van de optie 31[79]. Het betekent dat er geen massa vergelijkingen plaatsvinden tussen de door de *ANPR* gecapteerde gegevens en de DIV op basis van tekstbestanden. Deze wijze van verwerking draagt bij aan het gegevensbeschermingsniveau (voorkomen van massale datalekken).

47. De PZ heeft op dit moment geen zicht op de aantallen entiteiten waarvoor de PZ verantwoordelijke eenheid is, noch op het aantal mogelijke fouten per geïdentificeerde entiteit in de ANG. **Dat vertaalt zich onder meer in het gegeven dat er momenteel geen zicht is op het aantal te nemen maatregelen waardoor ook een kwaliteitscontrole op zaken zoals einddatum of relevantie niet mogelijk is**. Dit heeft dan weer mogelijke implicaties voor het correct uitvoeren van maatregelen op het terrein, al dan niet onder de vorm van correlaties via de ANPR werking. In het belang van een structurele kwaliteitscontrole van de ANG met betrekking tot de entiteiten waarvan de PZ de verantwoordelijke eenheid is, is de PZ vragende partij voor het ter beschikking stellen van een duidelijk dashboard dat per parameter de aantallen alsmede de technische sleutels ter controle toont.

48. Niettemin stelde het COC vast dat de PZ een visie hanteert die duidelijk conform de MFO3 en het 'Vademecum Gerechtelijke Politie' verloopt. Zo wordt er geen gebruik maakt van een PV (proces-verbaal) met parketcode 45 voor verdachte handelingen, maar wel van het concept van de RIR[80]. Er wordt ook geen gebruik gemaakt van het basisregistratiecriterium 'onderzoekselement' voor de binding tussen entiteiten en concrete feiten. De visie inzake bindingen tussen entiteiten en onderzoeken stemt volledig overeen met de logica dienaangaande: geen binding meer tussen entiteiten en een afgesloten onderzoek tenzij de binding door een concreet feit kan worden hardgemaakt.

49. Het COC stelde bij de PZ ook een bezorgdheid vast over de kwaliteit van de gegevens afkomstig van een andere gegevensbank[81]; zo zouden er problemen opduiken met de correctheid van de namen, voornamen, geboortedata en nationaliteit. Uit een expliciete vraag van het Controleorgaan met betrekking tot het gebruik van een specifiek bij naam genoemde databank meent het COC eveneens enige bezorgdheid te kunnen detecteren. Het Controleorgaan vermoedt dan ook, dat het gebruik van deze databank en de daaraan gekoppelde processen een negatieve invloed zou kunnen hebben op de correcte weergave van de onderzoeken in de ANG, waardoor de coördinatie van onderzoeken wordt bemoeilijkt in de SICAD-AIK werking. Het COC zal zich over deze verwerkingen informeren en een onderzoek opstarten.

50. Er is een duidelijke visie inzake de raadplegingen van de ANG. Het profiel NKF[82]is voorbehouden voor leden van de lokale recherchedienst (LRD) en leden van het functioneel beheer. Een aantal hoofdinspecteurs van de andere diensten beschikt ook over dit profiel doch heeft daarvoor een duidelijke opleiding gekregen. Er wordt volgens de PZ ook ingezet op het invullen van een duidelijke reden raadpleging[83]. De PZ heeft weliswaar geen beleidsdocument ter zake overlegd. Er werd enkel verwezen naar een recente instructie van de korpschef[84]. Het COC heeft tijdens het plaatsbezoek op dat vlak geen steekproef uitgevoerd.

51. Voor de controles op het terrein wordt er in eerste instantie uitgegaan van de 'ANG controle' voor een aftoetsing van de te nemen maatregelen. Er kon vastgesteld worden dat de politie duidelijk blijk geeft van kennis over de wijze

[78] De optie 35 is politiejargon voor het uitvoeren van de flux van de basisgegevensbanken naar de ANG.
[79] De optie 31 is politiejargon voor het uitvoeren van een bulkbevraging van de DIV op basis van een lijst van captaties uit een technische gegevensbank ANPR die verkregen werd d.m.v. een *querie*.
[80] 'Verdachte handelingen' zijn eigenlijk zachte (niet concrete) gegevens die door ze te verwerken op de wijze van een PV parket code 45 'Verdachte Handelingen' in de ANG oneigenlijk de status van concrete gegevens met de daarbij horende bewaartermijn krijgen.
[81] Dit betreft een nieuw digitaal communicatie- en informatieplatform voor de opvolging van personen die vrij zijn onder voorwaarden.
[82] Voor de bevragingen van de ANG Consultatie wordt het onderscheid gemaakt tussen het profiel basisexploitatie (informatie gelinkt aan concrete feiten) en gevorderde exploitatie (informatie gelinkt aan niet-concrete feiten en onderzoeken). Het gebruik van dit laatste profiel impliceert een doorgedreven kennis van de gebruikte concepten in de ANG om een correcte interpretatie van de resultaten van een bevraging te kunnen geven. De politiezones zijn verantwoordelijk voor het beheer en het nazicht van de toegangen tot de ANG waarover de onder hun verantwoordelijkheid ressorterende personeelsleden beschikken. Het profiel NKF ('Niet Konkreet Feit'; het woord 'konkreet' is oude spelling maar de afkorting wordt om technische redenen gehandhaafd) laat toe om meer informatie te verkrijgen, doch een niet correct gebruik op het terrein kan schade toebrengen aan lopende onderzoeken.
[83] Het betreft een e-mail van de korpschef van 1 september 2020 naar het politiepersoneel in het voortuitzicht van de visitatie van het COC.
[84] Het betreft een e-mail van de korpschef van 1 september 2020 naar het politiepersoneel in het voortuitzicht van de visitatie van het COC.

waarop een bevraging in de ANG best dient te gebeuren. Tot slot maakt de politiezone gebruik van de beschikbare operationele tools .

52. Uit het voorgaande volgt dat er bij de PZ een goede kennis en visie is op het vlak van de ANG-werking en dat een dashboard ANG zoals het COC dat voor ogen heeft een goede ondersteuning zou zijn.

53. Er worden echter geen (periodieke) proactieve controles op eventuele onrechtmatige consultaties uitgevoerd. Het Controleorgaan wijst er op dat, naast de WGB, een omzendbrief van de procureur des Konings Oost-Vlaanderen bijvoorbeeld proactieve controles op de rechtmatigheid van de verwerkingen in de politionele databanken sedert 15 september 2017 uitdrukkelijk voorschrijft (Cf. OBOV 2017-016 van 7 september 2017 betreffende de "*Basisrichtlijnen inzake het consulteren van databanken*"): "*Binnen de onderscheiden politiediensten dienen er regelmatig (minstens halfjaarlijks) steekproefsgewijze controles te gebeuren op het rechtmatig gebruik van de databanken. Vastgestelde inbreuken op het beheer, toegang en gebruik van de databanken moeten onverwijld aan het openbaar ministerie worden gemeld. Inbreuken kunnen aanleiding geven tot strafrechtelijke en/of tuchtrechtelijke vervolging*" (p. 3).

In het licht van de vastgestelde tekortkoming dringt het Controleorgaan er op aan dat een policy/beleid wordt opgesteld dat voorziet in een mechanisme waardoor periodiek en effectief controles worden uitgevoerd op het monitoren van eventuele (on)rechtmatige consultaties mede gelet op de WGB en dit naar analogie met de door de procureur des Konings Oost-Vlaanderen opgelegd verplichting en *good practice*.

Corrigerende maatregel
Op regelmatige basis loggings op te vragen van de ANG en proactieve controles door middel van steekproeven (2 x/jaar) te houden met het doel toezicht te houden op het verplicht ingeven van een reden van raadpleging en op eventuele onrechtmatige consultaties en dit een eerste maal binnen de zes maanden na kennisname van deze corrigerende maatregel en de resultaten ervan ter beschikking te houden van het COC

4.2.2. De validatie van de gegevens (centrale validatie)

54. De gestructureerde geregistreerde gegevens moeten na voorbereiding in de lokale toepassing (ISLP,[85] Lokale vatting, …) overgemaakt worden aan het centrale niveau, waar ze automatisch gecontroleerd worden.

De PZ voerde tussen 01/01/2020 en 31/03/2020 in totaal ***61*** transferts van gegevens (Optie 35). Dit betekent dat er elke werkdag lokaal geregistreerde gegevens worden overgemaakt aan het centrale niveau. Dit is een **positieve vaststelling** aangezien er een continue voeding is naar het centrale niveau.

4.3. Bijzondere gegevensbanken

55. Vóór de invoering van de Wet Politioneel Informatiebeheer 2019[86]was er een uitdrukkelijke aangifteplicht van de bijzondere gegevensbanken bij het Controleorgaan. Sinds de inwerkingtreding van deze wet moet de bijzondere gegevensbanken in het register van verwerkingen worden opgenomen (zie rubriek 3.3.9)[87]. Het Controleorgaan stelt vast dat een reeks bijzondere gegevensbanken in het register zijn opgenomen. De PZ beschikt evenwel niet over een korpsorder waarin de omstandigheden en de voorwaarden voor het aanleggen en gebruik van een bijzondere gegevensbank zijn vastgelegd.

56. Zonder alle in het register vermelde bijzondere gegevensbanken aan een inhoudelijke toetsing te onderwerpen, is het COC van oordeel dat een aantal van de verwerkingsactiviteiten bezwaarlijk onder een bijzondere gegevensbank vallen. Als voorbeelden kan het bewaren van de volgende gegevens worden genoemd: een register van evenementen, aanvragen in het kader van het toegangsbeheer tot politionele gegevensbanken en een bijzondere gegevensbank voor 'COVID 19 dossiers'. Deze laatste in een bijzondere gegevensbank bewaren is bijzonder vreemd omdat voor de

[85] *Integrated System for the Local Police*.
[86] Wet van 22 mei 2019 tot wijziging van diverse bepalingen van het politionele informatiebeheer, *BS* 19 juni 2019.
[87] Wet van 22 mei 2019 tot wijziging van diverse bepalingen wat het politionele informatiebeheer betreft. Art. 44/11/3, WPA *juncto* artikel 145 van wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus.

verwerking van deze processen-verbaal een afzonderlijk module in de ANG is voorzien. Het verwerken van deze gegevens in een bijzondere gegevensbank is bijgevolg strijdig met de bepalingen inzake het informatiebeheer voorzien in de WPA.

In antwoord op een opmerking van de PZ op het ontwerprapport merkt het Controleorgaan op dat niet-operationele verwerkingen niet onder de toepassing van de WPA vallen maar wel onder de AVG, zoals personeelsgegevens. Wat betreft de 'COVID 19 dossiers' stelt het Controleorgaan vast dat de politionele verwerkingen in dit raam kunnen verlopen aan de hand van de reguliere verwerkingsprocessen. Het Controleorgaan vraagt zich dan ook af wat onder de noemer van de bijzondere gegevensbank 'COVID' nog bijkomend zou moeten verwerkt worden.

Aanbeveling
Het COC dringt er op aan dat de PZ in een korpsorder een beleid uitstippelt voor het aanleggen van bijzondere gegevensbanken waarin parameters zijn opgenomen op basis waarvan kan afgetoetst worden of het aanleggen een bijzondere gegevensbank voor die welbepaalde verwerkingsactiviteit beantwoordt aan de wettelijke voorwaarden van artikel 44/11/3 WPA.

4.4. Het gebruik van mobiele toestellen al dan niet in het kader van operationele opdrachten en het gebruik van camerabeelden voor niet operationele doeleinden

57. In dat verband werden de volgende casussen aan de PZ voorgelegd:

1) het gebruik van een smartphone om vaststellingen te doen bij een zwaar verkeersongeval of inbraak;
2) de ICT-dienst meldt aan de korpschef een onverklaarbaar overmatig dataverbruik door het politiepersoneel. Welke procedure wordt er toegepast?;
3) een burger beweert dat hij door de politieambtenaar aan het onthaal niet adequaat werd bejegend. In het onthaal wordt gebruik gemaakt van vaste camera's;

58. Op het gebruik van privétoestellen voor operationele verwerkingen werd door de PZ geantwoord dat het gebruik van privétoestellen bij interventies niet is toegelaten. Deze casus zou zich nog niet hebben voorgedaan. Volgens de PZ wordt aan de politieambtenaar de nodige professionele toestellen ter beschikking gesteld.

59. In dat verband beschikt de PZ over twee korpsorders die respectievelijk betrekking hebben op "*algemene informatieveiligheid"* van 14 augustus 2020" en "*Policy Mobile Devices/FOCUS – regeling voor toekennen van smartphones en abonnementen*" van 11 september 2020[88]. Op de eerste en tweede casus biedt **de korpsorder "*algemene informatieveiligheid*" echter geen (afdoende) antwoord,** behalve dat de PZ het personeel een dienst- of bedrijfstoestel ter beschikking stelt en in 2020 *verplicht* wordt overgegaan tot het gebruik van de Focus-app die het mogelijk maakt om "*beelden door te sturen en incidenten op te volgen*". Het personeelslid kan er evenwel ook voor kiezen om zijn eigen toestel te gebruiken maar ook op het persoonlijk toestel moet de Focus-app geïnstalleerd worden**.**

60. In de korpsorder "*Algemene informatieveiligheid"* wordt een rubriek gewijd aan "*Gebruik van commerciële internetdiensten en publieke clouds*"[89]. Er wordt gesteld dat "*de politiemedewerkers* (*kunnen*) *tijdens de uitoefening van hun taken geen gebruik maken van commerciële internetdiensten en publieke clouds zoals Whatsapp, Facebook (…) met uitzondering van nooddiensten*", omdat deze diensten onvoldoende garanties bieden dat de GDPR[90]wordt nageleefd. Daarna wordt kort een rubriek gewijd aan "*Externe communicatie, internetpatrouille en onlinerecherche*". Er wordt gesteld: "*De geïntegreerde politie kan nog wel gebruik maken van allerlei commerciële internetdiensten voor doeleinden waarbij wij als organisatie geen persoonsgegevens verwerken*[91]*. Enkele voorbeelden hiervan zijn:*
- Externe communicatie via korpsprofiel op bijvoorbeeld Facebook of Twitter.
- Gebruik van profielen op sociale media in het kader van internetpatrouille of recherche"[92].

[88] Dienstorder nr. 12/2018.
[89] Rubriek 7, p. 13.
[90] Algemene Verordening Gegevensbescherming, of AVG.
[91] Onderlijning COC.
[92] Rubriek 7.2., p. 14.

61. In de eerste plaats blijkt dat door het samen lezen met de voorgaande rubriek het voor de politieambtenaar (en het COC) niet duidelijk, minstens verwarrend, is in welke gevallen de politieambtenaar nu al dan niet mag gebruik maken van sociale media waarbij informatie en persoonsgegevens worden verwerkt met een operationeel karakter. In de tweede plaats is het evident niet juist dat de politie geen persoonsgegevens zou verwerken wanneer zij participeert op sociale media[93].

62. Wat de controle op het overmatig dataverbruik betreft (2de casus) blijkt uit de antwoorden dat door de **PZ een procedure wordt gevolgd die een afspiegeling of analoge toepassing is van de principes van de collectieve arbeidsovereenkomst (CAO) nr. 81 met betrekking tot de controle op het gebruik van het internet**[94]**.** Deze CAO is algemeen bindend verklaard, waardoor deze van toepassing is voor alle werkgevers in de private sector en dus niet van toepassing op de overheidsdiensten, zoals de GPI. Deze CAO nr. 81 bevat evenwel de basisprincipes van het persoonsgegevensbeschermingsrecht (AVG) waardoor niets eraan in de weg staat dat de politie voor het invoeren van controles op de werkplaats bij de basisvoorwaarden van deze CAO nr. 81 aansluit of deze naar analogie toepast. Hetzelfde geldt voor de derde casus waarbij de camerabeelden die initieel voor politionele doeleinden (WPA) werden gebruikt, ook in een arbeidsrechtelijke context (AVG-doeleinden) kunnen worden aangewend. **Voor het COC is die basishouding zonder meer een *best practice*.**

63. Van belang is evenwel dat de PZ in een korpsorder de procedure uitwerkt waarbij de basisprincipes op een transparantie wijze concreet worden uitgewerkt: doeleinden, noodzakelijkheid en proportionaliteit, gevolgen voor de betrokkene en de rechten van de betrokkene[95]. Het gebruik van politionele gegevens in de arbeidsverhouding brengt met zich dat op deze verdere verwerking de AVG van toepassing is (transparantie en rechten van de betrokkene). Dat geldt eveneens wat betreft het gebruik van operationele camerabeelden voor de controle op de naleving van de arbeidsvoorwaarden. In dat verband verwijst het Controleorgaan naar zijn advies uit eigen beweging van 17 augustus 2020 "*met betrekking tot het invoeren van camerabewaking door de geïntegreerde politie met het oog op de controle van de naleving van de arbeidsvoorwaarden*" (BD200007) dat als leidraad kan dienen[96].

Aanbeveling

Het is van belang dat de korpschef in het korpsorder duidelijk onderscheid maakt tussen de diverse aspecten die worden beoogd op het vlak van de toegang tot en het gebruik van het internet en van sociale media voor persoonlijke en professionele doelstellingen en al dan niet gebruik van persoonlijke toestellen[97]. Zo moet de toegang tot het internet (zoekopdrachten, toegelaten en verboden websites) tijdens de diensturen worden onderscheiden van het gebruik van sociale media tijdens de diensturen voor persoonlijke doeleinden, enerzijds, en voor zover politionele informatie zou kunnen gedeeld worden, anderzijds. In een apart luik of afzonderlijk document wordt het gebruik van mobiele privétoestellen voor operationele doeleinden en het gebruik van professionele mobiele toestellen voor persoonlijke doeleinden (afzonderlijk) beschreven. Het is daarbij van belang dat het document duidelijk beschrijft wat toegelaten of verboden is, in welke omstandigheden en onder welke voorwaarden controle kan uitgevoerd worden, wat de gevolgen zijn wanneer inbreuken op het document worden vastgesteld en wat in dat verband de rechten van de betrokkene zijn. Het is dus van belang dat een duidelijk onderscheid wordt gemaakt tussen de diverse aspecten en doeleinden waarbij een procedure wordt uitgetekend waarin de basisprincipes van transparantie en rechten van de betrokkene concreet worden uitgewerkt. Dat is eveneens het geval wat betreft het gebruik van operationele camerabeelden voor de controle op de naleving van de arbeidsvoorwaarden.

4.5. Gegevensbescherming

4.5.1. Het verwerken van biometrische gegevens voor niet-operationele doeleinden

[93] Bovendien is het niet in alle gevallen uitgesloten dat ook de gebruiker als (gezamenlijke) verwerkingsverantwoordelijke moet worden beschouwd (zie HvJ, 29 juli 2019, Fashion ID, C-40/17).

[94] CAO nr. 81 Collectieve arbeidsovereenkomst nr. 81 van 26 april 2002, gesloten in de Nationale Arbeidsraad, "*tot bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de controle op de elektronische on-line communicatiegegevens*".

[95] Wat de camerabewaking betreft, zie het advies van het COC uit eigen beweging van 17 augustus 2020"*met betrekking tot het invoeren van camerabewaking door de geïntegreerde politie met het oog op de controle van de naleving van de arbeidsvoorwaarden*" (BD200007), https://www.controleorgaan.be/nl/publicaties/adviezen-aanbevelingen.

[96] www.controlergaan.be/publicaties/adviezen/aanbevelingen.

[97] Het Controleorgaan vestigt daarbij de aandacht op wettelijke regelingen die de vertrouwelijkheid van privécommunicatie beschermen, zoals artikel 314bis van het Strafwetboek en de wet van 13 juni 2005 betreffende de elektronische communicatie (BS 20 juni 2005) die de vertrouwelijkheid van de telecommunicatie beschermt (artikel 5 van deze wet).

64. De PZ maakt met het oog op de tijdsregistratie van de personeelsleden[98]en toegangscontrole geen gebruik van vingerafdrukken. Op het vlak van het gebruik van mobiele toestellen wordt in de korpsorder *Mobile Devices*, rubriek 4.1.1. 'Wachtwoord' (pagina 12), het volgende gesteld: "*Zowel voor de dienst- en bedrijfstoestellen als voor de privétoestellen (BYOD) dient de ontgrendelingsmethode met biometrie te gebeuren indien het toestel deze mogelijkheid biedt. Er dient een sterk wachtwoord ingesteld te worden als back-up of als biometrisch ontgrendelen niet mogelijk is*". Volgens de PZ gaat het echter niet om een verplichting noch kan de toepassing van een biometrische ontgrendeling van de dienst- en bedrijfstoestellen door de PZ gecontroleerd worden. Het COC verwijst naar de hiervoor opgemerkte inconsistenties (zie de randnummers 60 en 61) in de korpsorders en de toepassing ervan in de praktijk.

65. Volledigheidshalve verstrekt het COC toelichting over de reden van deze vraag aan de politiezones en het standpunt van het COC. De registratie van de gebruiker in het systeem gebeurt door het verzamelen van de relevante biometrische kenmerken van die persoon die gekoppeld worden aan de gegevens bij de personeelsdienst. De voornaamste reden[99]voor het invoeren van het controlesysteem betreft het aspect van authenticatie, met name dat degene die zich registreert wel degelijk de persoon is met wie de identificatiegegevens overeenstemmen. Hoewel het uitgangspunt doorgaans is dat alle personeelsleden voor de tijdsregistratie gebruik maken van de vingerafdrukken, kan toch – bij wijze van alternatief - gebruik worden gemaakt van de persoonlijk badge.

66. Het systeem werkt als volgt. Voor het vastleggen van de gegevens van de betrokkene in het systeem wordt eerst een beeld van de vingerafdruk gegenereerd. Met behulp van een speciaal algoritme, waardoor de vingerafdrukken worden omgezet in een unieke code die vervolgens op een *Record*, de *template*, wordt opgeslagen. Het lezen van de biometrische kenmerken van de betrokkene gebeurt door een vergelijking van de vingerafdrukken met de opgeslagen gegevens (*matching*) op de *template*. Hoewel de vingerafdrukken als zodanig niet wordt opgeslagen, worden de biometrische gegevens omgezet in een unieke code op basis waarvan de betrokkene wordt geïdentificeerd (een centraal systeem van de personeelsdienst). **Deze unieke code bevat dus de cijfermatige weergave van de vingerafdrukken, die ontegensprekelijk betrekking hebben op de biometrische persoonsgegevens van de betrokkene. Of de vingerafdruk nu 'in klaar' of in '*template*' of 'sjabloon' (die unieke code) bewaard wordt maakt geen verschil uit: het zijn en blijven biometrische gegevens.**

4.5.2. De toestemming

67. De toestemming als juridische grondslag (art. 9.2 a) AVG) is niet aanvaardbaar gezien het ondergeschikte verband en de gezagsverhouding. **De toestemming van een personeelslid van de geïntegreerde politie is *in casu* nooit echt "vrij" in de zin van het gegevensbeschermingsrecht.** Ook wanneer een alternatief wordt aangeboden (zoals *in casu* het stamnummer opgeslagen in de badge) blijft de toestemming als wettelijke grondslag voor het verwerking van de vingerafdrukken kaduuk.

4.5.3. Zwaarwegend algemeen belang

68. Als wettelijke grondslag is er nog art. 9.2 g) van de AVG dat de verwerking van biometrische gegevens toelaat indien "*de verwerking noodzakelijk* (is) *om redenen van zwaarwegend algemeen belang, op grond van Unierecht of lidstatelijk recht, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene*". **Dergelijke internrechtelijke bepaling of rechtsbasis is in België niet voorhanden**.

4.5.4. Verplichtingen van de verwerkingsverantwoordelijke (de korpschef)

69. Een laatste optie lijkt artikel 9.2 b) van de AVG en met name dat de verwerking "*noodzakelijk (is) met het oog op de uitvoering van verplichtingen en de uitoefening van specifieke rechten van de verwerkingsverantwoordelijke of de betrokkene op het gebied van het arbeidsrecht en het sociale zekerheids- en sociale beschermingsrecht, voor zover zulks is toegestaan bij Unierecht of lidstatelijk recht of bij een collectieve overeenkomst op grond van lidstatelijk recht die passende waarborgen voor de grondrechten en de fundamentele belangen van de betrokkene biedt*". **Opnieuw is een dergelijke internrechtelijke bepaling of rechtsbasis in België niet voorhanden.** Een collectieve arbeidsovereenkomst is evenmin mogelijkheid gezien we ons bevinden in overheidsverband. M.a.w. zelfs indien er een

[98] Zowel politieambtenaren als CALOG-personeel.
[99] Er wordt ook verwezen naar efficiëntiewinst op het vlak van personeelsadministratie.

collectief akkoord zou zijn met het personeel (vakbonden) vormt dit geen afdoende rechtsbasis omdat, naar Belgisch recht, een akkoord met de vakbonden in de sector van de politie geen afdwingbare juridische norm is. Hoe dan ook zou dergelijke collectieve overeenkomst dan sowieso "*passende waarborgen voor de grondrechten en de fundamentele belangen van de betrokkene"* moeten bieden.

70. Het COC heeft in dat verband ook het advies ingewonnen van de federale politie, directie-generaal van het middelenbeheer en de informatie (DGR). Hierna volgt de letterlijk de visie weer van DGR, met de in "**vet**" vermelde passage, die de essentie ervan naar het inzicht van het COC weergeeft en waaruit blijkt dat ook DGR zich aansluit bij de visie van het COC.
"Faisant suite à votre mail du 28 mars 2019, vous trouverez ci-après la position du service juridique de la police fédérale. Cette position a été concertée avec les différentes entités en charge de l'interprétation et de l'application de la réglementation en matière de protection des données.
L'article 9.2 b) du RGPD exige qu'un traitement de données considérées comme sensibles soit autorisé « par le droit d'un État membre ou par une convention collective conclue en vertu du droit d'un État membre qui prévoit des garanties appropriées pour les droits fondamentaux et les intérêts de la personne concernée ».
Le statut syndical (réf. 2) pose le principe de la négociation préalable avec les organisations syndicales représentatives lors de l'adoption de réglementations de base ayant trait au statut policier, et érige par ailleurs le comité de négociation en organe d'avis des ministres de tutelle. Il s'agit, pour l'autorité, de consulter et d'informer les représentants des membres du personnel de ses intentions. La négociation constitue donc une "étape de procédure" dans l'adoption de textes légaux et réglementaires statutaires.
Le protocole qui résulte des négociations syndicales ne créé pas une « règle de droit » contenant des droits et obligations pour les membres du personnel et ne constitue par conséquent pas, en lui-même, un fondement suffisant au sens de l'article 9.2 b) du RGPD. A l'instar des conventions collectives dans le secteur privé, lesquelles sont rendues obligatoires par arrêté royal, un accord syndical doit, selon nous, être formalisé dans un instrument légal ou réglementaire afin de répondre aux exigences du règlement européen.
Pour votre information complète, une vision intégrée concernant l'utilisation des empreintes digitales dans le cadre de l'application du statut est en cours de réflexion au sein de la police intégrée, afin d'uniformiser les pratiques en la matière. Cette vision intégrée ne fera pas l'économie d'une analyse de la subsidiarité et de la proportionnalité d'un tel traitement de données à caractère personnel au regard des finalités poursuivies, tandis que les garanties appropriées devront être déterminées ».

71. In aansluiting met van bovenstaande analyse, is het Controleorgaan, voor zoveel als nodig, van oordeel dat een verslag BOC en/of het advies van de GBA bezwaarlijk als rechtsbasis aangenomen kunnen worden. Zo wordt in het verslag BOC op geen enkele wijze allusie gemaakt op het feit dat een controlesysteem met vingerafdrukken zou worden ingevoerd, laat staan dat een wettelijke basis wordt aangeduid. Wat het advies van de GBA betreft moet aangestipt worden dat het advies werd uitgebracht in 2008, onder de toepassing van de inmiddels opgeheven wet van 8 december 1992 betreffende de verwerking van persoonsgegevens waarin de verwerking van biometrische gegevens niet was geregeld. Bovendien, indien al rekening zou gehouden kunnen worden met het advies – quod non - acht de GBA het invoeren van het systeem slechts in uitzonderlijke gevallen aanvaardbaar. Er mogen geen andere minder privacy-ingrijpende maatregelen tot hetzelfde resultaat kunnen leiden en het moet gaan om plaatsen met een bijzonder (hoog) veiligheidsrisico. Dat de verwerking van de vingerafdrukken door de PZ niet pertinent is, blijkt reeds uit de mogelijkheid die wordt geboden om zich toch aan de hand van de persoonlijke badge te registreren.

72. Het voorgaande brengt het Controleorgaan tot de conclusie en slotsom dat een systeem van vingerafdrukken van het personeel voor de vermelde finaliteit *de lege lata* **niet wettelijk** is.

4.5.5. Het register van verwerkingen

73. De PZ heeft een register van verwerkingen.

4.6 Functionaris voor gegevensbescherming (DPO)

74. De politiezone maakt gebruik van een functionaris voor de gegevensbescherming (*DPO*) die op provinciaal niveau (een koepel) is aangewezen[100]en een assistent *DPO* die op korpsniveau is aangewezen. Beiden behoren tot het administratief kader (CALOG-personeelslid). De provinciale *DPO* oefent haar functie van *DPO* voltijds uit, maar werkt in deze hoedanigheid ten behoeve van meerdere politiezones, waaronder dus ook de PZ[101]. De provinciale *DPO* staat evenwel in voor de coördinatie van niet minder dan 14 politiezones, waarvan 6 politiezones over een assistent *DPO* beschikken. In de PZ wordt de provinciale *DPO* dus bijgestaan door een lokale contactpersoon.

75. Hoewel de *DPO* inderdaad voor verschillende politiezones kan aangesteld worden, moet zorg worden gedragen dat die zijn opdrachten effectief en efficiënt kan uitvoeren. Een *DPO* dient over voldoende tijd en middelen te beschikken om zijn functie te kunnen uitoefenen. De notie "*voldoende beschikbare tijd*" staat nergens gedefinieerd. De *DPO* zal dus in functie van elke situatie moeten worden beoordeeld, met dien verstande dat de *DPO* zich daadwerkelijk van zijn taak kan kwijten. De functie van *DPO* is dus niet noodzakelijk een voltijdse tijdsbesteding. In dat verband moet de *DPO* kunnen beschikken over de informatie die nodig is voor de uitvoering van zijn of haar taken en heeft daartoe toegang tot de verschillende informatiekanalen en besluitvormingsorganen binnen de politiezone om hem of haar zo nauw mogelijk bij de werkzaamheden van de politiezone te betrekken. Gelet op het multidisciplinaire karakter van gegevensbescherming en informatieveiligheid en de zeer specifieke expertise en competenties waarover een *DPO* dient te beschikken, is het Controleorgaan er zich terdege van bewust dat het voor een politiezone geen evidente zaak is om binnen de eigen organisatie altijd een geschikte kandidaat aan te duiden die deze functie op zich neemt (gaande van een beperkt aantal uren per week/deeltijds tot mogelijks voltijds) en om tevens hiervoor de nodige middelen (tijd/geld) te voorzien om zijn/haar expertise verder op te bouwen en te onderhouden.

76. Het Controleorgaan stelde vast dat de PZ beroep doet op een *DPO* die over de vereiste competenties beschikt en de functie voltijdse uitoefent, verdeeld over meerdere politiezones. In totaal betreft het hier veertien (14) politiezones. Het aantal uur per week (of uitgedrukt in het percentage VTE) dat *DPO* wijdt aan zijn functie van coördinerend *DPO* voor de PZ is niet vastgelegd. Er werd door de *DPO* geargumenteerd dat haar tijdsbesteding per korps onmogelijk te bepalen valt; zij verdeelt de beschikbare tijd naar best vermogen over de verschillende politiezones. Zodoende kan zij haar aandacht volledig toespitsen op deze materie en aldus haar deskundigheid en (praktijk)kennis in het domein van gegevensbescherming verder uitbreiden en onderhouden.

77. Eenzelfde persoon mag dus weliswaar diensten verstrekken aan meerdere politiezones, maar het aantal uren per week dat zij daadwerkelijk als *DPO* voor een politiezone optreedt, moet vanzelfsprekend realistisch zijn om de functie naar behoren te kunnen uitvoeren. Het Controleorgaan is van oordeel dat een *DPO* minstens vier uren per week als dusdanig actief moet zijn voor diezelfde politiezone, tenzij ten opzichte van het Controleorgaan afdoende kan worden aangetoond dat dit niet noodzakelijk is of zou zijn. Het totaal aantal uren per week (de som van het aantal uren per week in elke betrokken politiezone) mag in geen geval de veertig (tijd voorzien voor 1 VTE) overschrijden. Gelet op de omvang van haar coördinerende functie (14 PZ's waarvan 6 ook een eigen (assistent) hebben) lijkt het zeer twijfelachtig of de *DPO* voor de PZ voldoende tijd kan besteden aan haar wettelijke opdrachten.

In tegenstelling tot wat de PZ in het antwoord op het ontwerprapport uit het bovenstaande randnummer meent te moeten afleiden, gaat het om een *gemiddelde* van minstens vier uren per week *verspreid* over alle werkzaamheden of taken die de DPO in een politiezone besteedt.

78. Uit de antwoorden op de toegestuurde vragenlijst, de interviews afgenomen tijdens het plaatsbezoek en uit de actuele lijst van nog te ondernemen acties m.b.t. gegevensbescherming (verder uitwerken, actualiseren en implementeren van een beleid inzake gegevensbescherming en informatieveiligheid, uitvoeren van *DPIA's*, continu inzetten op bewustmaking, …), **komt het Controleorgaan tot de vaststelling dat de coördinerende *DPO* voor de PZ, gelet op de beperkte tijdsbesteding, eerder op specifieke aanvraag van de PZ ten gronde betrokken is bij de implementatie, het dagelijkse beheer en opvolging van het beleid inzake gegevensbescherming en informatieveiligheid,** waardoor er sprake is van een verhoogd risico dat zij geen of niet tijdig adviezen verstrekt omtrent gegevensverwerkende activiteiten en haar rol ten volle kan opnemen. De *DPO* treedt eerder op als expert (o.a. opmaak template documenten, aanreiken methodologieën, …) en als coach voor de interne contactpersoon/coördinator gegevensbescherming.

[100] Art. 144 Wet Geïntegreerde Politie en de artikelen 63, 64 en 65 WGB
[101] Zoals voorzien in artikel 144,tweede lid, Wet Geïntegreerde Politie.

79. **Het Controleorgaan kon bijgevolg niet vaststellen dat de *DPO* voldoende de verwerkingsactiviteiten van de politie van opvolgt of kan opvolgen om hun conformiteit met de gegevensbeschermingswetgeving na te gaan.** De *DPO* moet immers ook proactief bij alle zaken rond gegevensverwerking betrokken worden, dit vereist tevens een actievere rol van het management.

Aanbeveling
Het Controleorgaan dringt aan op een bijsturing van de tijdsbesteding voor de DPO van de PZ en op het beperken van het aantal politiezones waarvoor zij tevens optreedt als DPO. Het COC is van oordeel dat de DPO in de huidige omstandigheden niet over voldoende middelen (tijd) kan beschikken om de taken van een DPO adequaat uit te voeren voor het grote aantal politiezones.

In de PZ is een officieel samenwerkingsverband opgezet tussen verschillende politiezones wat alleen maar kan toegejuicht worden. Dit zou in principe enkel maar de coherentie en de efficiëntie van het gegevensbeschermingsbeleid kunnen bevorderen. Maar ook in het kader van een samenwerkingsverband dient de PZ ervoor te zorgen dat er voldoende middelen worden voorzien zodat het takenpakket van de *DPO* naar behoren kan worden uitgevoerd. Hoe dit in de praktijk wordt gerealiseerd, is een keuze van de verwerkingsverantwoordelijke. De *DPO* mag ondersteund worden door een team om zijn takenpakket uit te voeren. De *DPO* en zijn/haar team fungeren als contactpunt binnen de PZ voor alle kwesties inzake de naleving van gegevensbeschermingswetgeving en dienen dus nauw betrokken te worden bij de verwerkingsactiviteiten van de politiezone.

80. Hierbij aansluitend is het COC van oordeel dat, ook al zijn er binnen de betrokken PZ één of meerdere lokale contactpersonen aangeduid en gevormd ter ondersteuning van de *DPO* voor de praktische coördinatie, opvolging en implementatie van het beleid en de processen inzake gegevensbescherming en informatieveiligheid, een (heel) beperkte tijdsbesteding voor een *DPO* (i.e. een beperkt aantal uren per week) enkel werkbaar/haalbaar kan zijn onder een aantal randvoorwaarden, met name:

- de *DPO* kan het wettelijk takenpakket (artikel 39 van de AVG en artikel 65 WGB) naar behoren uitvoeren. Het betreft hier dus:
    - bijstand en advies verlenen m.b.t. alle aspecten van gegevensbescherming,
        - in het bijzonder m.b.t. de gegevensbeschermingseffectbeoordelingen en de opmaak van het register van de verwerkingsactiviteiten;
        - in het bijzonder met betrekking tot eventuele *data breaches*;
    - het toekijken op de naleving van de gegevensbeschermingswetgeving (AVG, WGB, WPA) en van de interne regels rond gegevensbescherming;
    - contactpunt zijn voor de toezichthoudende autoriteit en hiermee samen werken;
    - fungeren als contactpersoon van de politiezone voor alle aspecten van gegevensbescherming (inclusief informatieveiligheid), zowel voor interne medewerkers als externe betrokkenen;
- er is reeds een zekere bewustwording aanwezig in alle lagen van de organisatie rond het belang van een adequaat gegevensbeschermingsbeleid;
- de *DPO* wordt actief betrokken bij de werkzaamheden van de PZ en geïnformeerd over alle gegevensverwerkende activiteiten zodat hij tijdig de nodige adviezen kan verlenen.

In antwoord op het ontwerprapport merkt de PZ op dat de bijstand bij het opmaken van het register van verwerkingsactiviteiten geen wettelijke verplichting is (artikel 39 AVG en 65 WGB). Het Controleorgaan merkt op dat de bijstand en adviesverlening van de DPO in verband staan met de verwerking van persoonsgegevens, ongeacht de vraag wie (functie/profiel) het verwerkingsregister moet opmaken en actualiseren.

4.7 Informatieveiligheid

4.7.1. Beleid en organisatie

81. Voor wat betreft de uitwerking van het beleid inzake informatieveiligheid en gegevensbescherming is het Controleorgaan er zich van bewust dat het 'beleid' een ruim concept is dat geconcretiseerd zou kunnen worden in een huishoudelijk reglement of dienstorder(s).

De PZ beschikt in dit verband over de volgende basisdocumenten:

- Korpsorder- Algemene informatieveiligheid (uitgiftedatum 31 januari 2019);
- Korpsorder - Korpsgewoontes voor de informatieveiligheid (uitgiftedatum 14 augustus 2020);
- Korpsorder - Omgaan met politionele informatie en databanken (uitgiftedatum 31 januari 2019);
- Korpsorder - Policy Telewerken (uitgiftedatum 11 september 2020);
- Korpsorder - Gebruik van *Office 365* GPI en *Sharepoint* (uitgiftedatum 31 januari 2019);
- Korpsorder - *Policy Mobile Devices*/FOCUS – regeling voor toekenning en gebruik van *smartphones* en abonnementen (uitgiftedatum 11 september 2020).

82. Het korpsorder "*Algemene Informatieveiligheid*" kan worden beschouwd als het korpsbeleid inzake informatieveiligheid: het beschrijft o.a. de rollen en verantwoordelijkheden van alle medewerkers en leidinggevenden m.b.t. informatieveiligheid, de aanstelling van een *DPO*, een data classificatiemodel (publiek, intern, beperkt) en een aantal na te leven richtlijnen en procedures. In dit beleidsdocument wordt voor een aantal specifieke onderwerpen verwezen naar aparte korpsrichtlijnen (bijvoorbeeld korpsnota "*Omgaan met politionele informatie en databanken*"). Er werd vastgesteld dat de vermelde korpsnota "*Omgaan met ICT-middelen*" nog in voorbereiding is.

Zoals hiervoor gesteld heeft het COC vastgesteld dat er bepaalde discrepanties tussen de documenten zijn. Dit is grotendeels te wijten aan de algemeenheid van de documenten in die zin dat ze niet volledig zijn afgestemd op de specifieke organisatie van de politiezone.

83. Het Informatieveiligheidsbeleid werd nog niet geconcretiseerd in een door de korpschef goedgekeurd informatieveiligheidsplan[102]. Maturiteitsmetingen en/of formele risicoanalyses m.b.t. informatieveiligheid en gegevensbescherming worden niet op periodieke basis uitgevoerd. Het COC kon geen formele benadering vaststellen voor risicobeoordeling en - beheersing met betrekking tot informatieveiligheid en in het bijzonder van persoonsgebonden informatie.

84. De PZ diende reeds onder de toepassing van het uitvoeringsbesluit van 6 december 2015 over een informatieveiligheidsplan te beschikken. Het betreft hier dus het opstellen, opvolgen en regelmatig bijwerken van een informatieveiligheidsplan, met daarin de prioriteiten, de verantwoordelijke(n) en de termijnen voor het realiseren van de voorgestelde maatregelen uit het plan. Dit plan wordt regelmatig herzien op basis van management besluiten, nieuwe risico's, gewijzigde wetgeving en andere organisatietaken.

Corrigerende maatregel
Er moet door de PZ een informatieveiligheidsplan opgemaakt worden. Het informatieveiligheidsplan wordt binnen de zes maanden na datum van kennisname van onderhavig rapport ter beschikking gesteld van het Controleorgaan.

Aanbeveling
Het wordt aanbevolen de volgende actiepunten op te nemen in het informatieveiligheidsplan:

- *de verdere uitwerking en verfijning van het beleid inzake informatieveiligheid en gegevensbescherming via korpsrichtlijnen en procedures. Dit beleid moet regelmatig door het management gerevalueerd worden zodat het relevant blijft, in lijn met de realiteit. Het is hierbij belangrijk om de uitgewerkte korpsnota's en procedures te communiceren, te duiden en regelmatig te herhalen (door middel van bewustmakingscampagnes).*
- *maturiteitsmetingen, risico- en kwetsbaarheidsanalyses zijn belangrijke pijlers in het beveiligingsbeleid en dragen bij tot een optimale risico-gebaseerde informatieveiligheid. De tijdsbesteding van de DPO is ook een onderdeel van dit risicobeheer;*
- *het opzetten van formele overleg- en communicatieprocedures met alle betrokken partijen binnen de PZ zodoende dat de DPO meer bij de werkzaamheden van de organisatie betrokken wordt en steeds over de nodige informatie beschikt voor de uitvoering van zijn opdracht die hem toevertrouwd werd.*

4.7.2. Logbestanden eigen ICT systemen ("traceerbaarheid")

[102] Met een informatieveiligheidsplan wordt hier bedoeld: een op een risicoanalyse gebaseerd plan om ontbrekende informatiebeveiligingsmaatregelen te implementeren zodat de veiligheidsobjectieven geformuleerd in het veiligheidsbeleid maximaal worden nagestreefd.

85. Uit de overgemaakte antwoorden en documentatie kon het COC niet vaststellen dat er voor diverse interne[103]ICT systemen en toepassingen wel logbestanden voorzien zijn teneinde de traceerbaarheid van acties te garanderen en incidenten retroactief te kunnen onderzoeken. Er is geen formeel beleid en documentatie rond het beheer van logbestanden (welke informatie wordt er gelogd, regels rond bewaartermijnen, toegangsmodaliteiten, enz. …). Er worden geen proactieve controles op de logbestanden uitgevoerd, dit gebeurt enkel op vraag (*ad hoc* basis). Er is geen gecentraliseerd log management platform of *SIEM*[104]tool voorzien. Het COC verwijst in dat verband naar de corrigerende maatregel in randnummer 36 in het kader van verwerkingen van persoonsgegevens, waarbij het beheer van logbestanden steeds de bepalingen van artikel 56 WGB dient te respecteren.

Aanbeveling
Het is aanbevolen om een risicoanalyse uit te voeren m.b.t. het beheer van logbestanden en het monitoren van de interne ICT-systemen teneinde de nodige garanties te bekomen rond de traceerbaarheid van gegevensverwerkende activiteiten.

4.7.3. Toegangsbeheer

86. M.b.t. het beheer van toegangen wenst het COC het belang te benadrukken van het gebruik van nominatieve accounts. Het gebruik van generieke account (bijv. dienstlogins die kunnen gedeeld worden tussen meerdere personen) dient vermeden te worden teneinde een correcte traceerbaarheid te garanderen m.b.t. gegevensverwerkende activiteiten. Ook gebruikers met uitgebreide toegangsrechten zoals systeem- en applicatiebeheerders (i.e. 'geprivilegieerde gebruikers') dienen hun dagdagelijkse systeemtaken uit te voeren d.m.v. een nominatief gebruikersaccount. Met gedeelde generieke accounts bestaat het risico dat bij misbruik niet te achterhalen valt wie daarvoor verantwoordelijk is. Bovendien kan een gecompromitteerde account van geprivilegieerde gebruiker, omwille van de uitgebreide toegangsrechten, in principe de sporen van activiteiten wissen door bijvoorbeeld de systeemlogbestanden aan te passen of deze geheel te wissen.

87. Er werden geen specifieke organisatorische of technische maatregelen voor het monitoren van geprivilegieerde gebruikers voorzien. Dit type van gebruikers zijn accounts met heel ruime toegangsrechten binnen een ICT systeem, toepassing, omgeving of domein (bijv. systeem- en applicatiebeheerders).

Aanbeveling
Het COC dringt er op aan om:

- *uitsluitend het gebruik van nominatieve/individuele gebruikersaccounts toe te laten in het kader van operationeel beheer. Het gebruik van een generiek gebruikersaccount voor systeembeheer dient sterk gelimiteerd te worden en wordt enkel toegelaten indien dit technisch vereist is;*
- *alle geprivilegieerde accounts te inventariseren, inclusief domein- en lokale accounts, om er zeker van te zijn dat alleen geautoriseerde personen verhoogde rechten hebben;*
- *ervoor te zorgen dat alle gebruikers met toegang tot een geprivilegieerde account een speciale of secundaire nominatieve account gebruiken voor het uitvoeren van ICT activiteiten waarvoor verhoogde rechten nodig zijn. Dit geprivilegieerde account mag alleen worden gebruikt voor deze administratieve activiteiten en niet voor het uitvoeren van de dagdagelijkse operationele activiteiten, surfen op het internet, e-mail of soortgelijke activiteiten;*
- *alle activiteiten m.b.t. het gebruik en het beheer van deze geprivilegieerde accounts op te nemen in logbestanden en integriteitsbeschermende maatregelen voor deze logbestanden te voorzien.*

4.7.4. Continuïteitsplanning

88. De PZ is gestart met het formuleren van een ICT continuïteitsplan waarin evenwel een aantal essentiële activa (o.a. servers en netwerk) nog niet geïntegreerd zijn. Het COC kon, op basis van de ontvangen informatiestukken, niet concluderen of er systematisch/op periodieke basis *DRP*/*BCM*[105]testen worden voorzien[106].

[103] Dus niet onder beheer van DRI.
[104] *Security Information and Event Management*.
[105] *Disaster Recovery Plan* (*DRP*)/*Business Continuity Plan* (*BCP*)
[106] Hieronder wordt onder meer begrepen: op periodieke basis testen van het *backup* beleid, simuleren van incidenten en crisissituaties (stroomonderbreking, uitvallen systeemcomponent, afwezigheid sleutelpersoneel, enz. …).

Aanbeveling
Het is aanbevolen een ICT noodvoorzieningsplan (DRP) en continuïteitsplan voor alle kritieke processen en essentiële informatiesystemen van de organisatie op te stellen en om dit op periodieke basis te testen. Een DRP voor ICT gaat veel verder dan louter een back-up voorzien. Het bereidt je als organisatie voor op alle mogelijke calamiteiten die de ICT-systemen kunnen ondervinden.

5. CONCLUSIE – AANBEVELINGEN – CORRIGERENDE MAATREGELEN

Conclusie

89. Een gering aantal aspecten van de gecontroleerde thema's blijken in overeenstemming met de wetgeving. Er werden een aantal wettelijke tekortkomingen vastgesteld. Wat betreft de aspecten met een duidelijke dominantie op het vlak van gegevensbescherming blijkt dat de PZ wel de ambitie heeft om antwoord te kunnen bieden op bepaalde gevoelige aangelegenheden, maar dit gedeeltelijk werd belemmerd door de geringe effectieve tijdsbesteding enerzijds en het gebrek aan uitvoerige documentatie van de daarmee samenhangende aspecten (ICT en informatieveiligheid) anderzijds, niettegenstaande het overduidelijk engagement bij de aangestelde personeelsleden en de *DPO*.

90. Voorgaande algemene vaststelling weerspiegelt de concrete vastgestelde tekortkomingen. Vooral op het domein van het gebruik van camerabewaking en de toepassing van het wettelijk kader met betrekking tot het gegevensbeschermingsrecht dient de kennis te worden aangescherpt en uitgediept. Diverse aspecten moeten in rekening worden gebracht: de belangen van zowel de politie als de betrokkene (de burger), de ernst van impact van het systeem op de persoonlijke levenssfeer van de betrokkene, het principe van *privacy by design*, gekoppeld aan een doorgedreven aandacht op het vlak van informatieveiligheid. Daarentegen heeft de PZ een zeer goede werking van het functioneel beheer.

91. Hoewel er een aantal korpsrichtlijnen m.b.t. informatieveiligheid werden opgesteld, heeft de PZ geen risico-gestuurd algemeen informatie veiligheids- en continuïteitsplan waarbinnen de organisatie, en in het bijzonder de ICT dienst, haar eigen maatregelen kan kaderen. Zo'n risico-gebaseerde aanpak zou toelaten om de genomen maatregelen te evalueren, te formaliseren en te documenteren. De ICT dienst van de PZ voorziet in een reeks ICT beveiligingsinitiatieven, maar het periodiek (intern/extern) nazicht van de goede werking en de volledigheid van deze initiatieven gebeurt niet op een structurele en formele wijze.

De betrokkenheid van de *DPO* bij het opvolgen, bijsturen en implementeren van het informatie veiligheids- en gegevensbeschermingsbeleid dient verhoogd te worden. Een structurele aanpak en periodieke opvolging zijn hier aangewezen.

Een reeks aanbevelingen dringen zich dan ook op die moeten bijdragen tot een verbetering van de efficiëntie en effectiviteit van de (persoons)gegevensverwerking door de PZ.

De vastgestelde wettelijke tekortkomingen nopen het Controleorgaan echter ook tot het nemen van corrigerende maatregelen waarbij de politiezone zich binnen een welbepaalde tijdspanne moet regulariseren.

OM DEZE REDENEN,

Het Controleorgaan op de Politionele informatie,

Vaardigt het hiernavolgende verzoek en de volgende aanbevelingen uit;

Neemt de hierna volgende corrigerende maatregelen,

Verzoekt,

de korpschef, in afwachting van het uitvoeringsbesluit inzake het lokaal cameraregister, een lokaal register van het cameragebruik aan te leggen of in een afzonderlijk luik in het register van verwerkingen op te nemen waarin de types van camera's, de doeleinden en het opslagmedium van de beelden duidelijk worden vermeld.

Aanbevelingen

1) Aanbeveling
Met het oog op een effectieve en efficiënte toepassing van de ANPR-verwerkingen is het van belang dat de PZ een duidelijk interventiebeleid voor de hits op nationale lijsten en een duidelijk actie- en interventiebeleid op de lokale lijsten uitwerkt.

2) Aanbeveling
Het Controleorgaan dringt er op aan dat een *policy*/beleid wordt opgesteld dat het mogelijk maakt een efficiënt mechanisme in plaats te stellen waarbij een continue monitoring gebeurt van de profielen en toegangen *in real time* kunnen beheerd worden in functie van de reële personeelsbezetting.

3) Aanbeveling
Het COC dringt er op aan dat de PZ in een korpsnota een beleid uitstippelt voor het aanleggen van bijzondere gegevensbanken waarin parameters zijn opgenomen op basis waarvan kan afgetoetst worden of het aanleggen van een bijzondere gegevensbank voor die welbepaalde verwerkingsactiviteit beantwoordt aan de wettelijke voorwaarden van artikel 44/11/3 WPA.

4) Aanbeveling
Het is van belang dat de korpschef in het korpsorder duidelijk onderscheid maakt tussen de diverse aspecten die worden beoogd op het vlak van de toegang tot en het gebruik van het internet en van sociale media voor persoonlijke en professionele doelstellingen en al dan niet gebruik van persoonlijke toestellen[107]. Zo moet de toegang tot het internet (zoekopdrachten, toegelaten en verboden websites) tijdens de diensturen worden onderscheiden van het gebruik van sociale media tijdens de diensturen voor persoonlijke doeleinden, enerzijds, en voor zover politionele informatie zou kunnen gedeeld worden, anderzijds. In een apart luik of afzonderlijk document wordt het gebruik van mobiele privétoestellen voor operationele doeleinden en het gebruik van professionele mobiele toestellen voor persoonlijke doeleinden (afzonderlijk) beschreven. Het is daarbij van belang dat het document duidelijk beschrijft wat toegelaten of verboden is, in welke omstandigheden en onder welke voorwaarden controle kan uitgevoerd worden, wat de gevolgen zijn wanneer inbreuken op het document worden vastgesteld en wat in dat verband de rechten van de betrokkene zijn. Het is dus van belang dat een duidelijk onderscheid wordt gemaakt tussen de diverse aspecten en doeleinden waarbij een procedure wordt uitgetekend waarin de basisprincipes van transparantie en rechten van de betrokkene concreet worden uitgewerkt. Dat is eveneens het geval wat betreft het gebruik van operationele camerabeelden voor de controle op de naleving van de arbeidsvoorwaarden.

5) Aanbeveling
Het COC dringt aan op een bijsturing van de tijdsbesteding voor de *DPO* en het beperken van het aantal politiezones waarvoor zij als *DPO* een coördinerende rol heeft, tenzij de assistent *DPO*'s daadwerkelijk hun taak op een zelfstandige wijze kunnen uitoefenen. Het COC is van oordeel dat de *DPO* in de huidige omstandigheden **niet** over voldoende middelen (tijd) kan beschikken om de taken van een *DPO* adequaat uit te voeren voor het grote aantal politiezones waarvoor zij aangesteld is.

6) Aanbeveling

Het wordt aanbevolen de volgende actiepunten op te nemen in het informatieveiligheidsplan:

- de verdere uitwerking en verfijning van het beleid inzake informatieveiligheid en gegevensbescherming via korpsrichtlijnen en procedures. Dit beleid moet regelmatig door het management gerevalueerd worden zodat

[107] Het Controleorgaan vestigt daarbij de aandacht op wettelijke regelingen die de vertrouwelijkheid van privécommunicatie beschermen, zoals artikel 314bis van het Strafwetboek en de wet van 13 juni 2005 "*betreffende de elektronische communicatie*" die de vertrouwelijkheid van de telecommunicatie beschermt (artikel 5 van deze wet).

het relevant blijft, in lijn met de realiteit. Het is hierbij belangrijk om de uitgewerkte korpsnota's en procedures te communiceren, te duiden en regelmatig te herhalen (door middel van bewustmakingscampagnes);
- maturiteitsmetingen, risico- en kwetsbaarheidsanalyses zijn belangrijke pijlers in het beveiligingsbeleid en dragen bij tot een optimale risico-gebaseerde informatieveiligheid. De tijdsbesteding van de DPO is ook een onderdeel van dit risicobeheer;
- het opzetten van formele overleg- en communicatieprocedures met alle betrokken partijen **binnen de PZ** zodoende dat de DPO meer bij de werkzaamheden van de organisatie betrokken wordt en steeds over de nodige informatie beschikt voor de uitvoering van de opdracht die hem toevertrouwd werd.

7) Aanbeveling
Het is aanbevolen om een risicoanalyse uit te voeren m.b.t. het beheer van logbestanden en het monitoren van de interne ICT-systemen teneinde de nodige garanties te bekomen rond de traceerbaarheid van gegevensverwerkende activiteiten.

8) Aanbeveling
Het COC dringt er op aan om:

- uitsluitend het gebruik van nominatieve/individuele gebruikersaccounts toe te laten in het kader van operationeel beheer. Het gebruik van een generiek gebruikersaccount voor systeembeheer dient sterk gelimiteerd te worden en wordt enkel toegelaten indien dit technisch vereist is.
- alle geprivilegieerde accounts te inventariseren, inclusief domein- en lokale accounts, om er zeker van te zijn dat alleen geautoriseerde personen verhoogde rechten hebben;
- ervoor te zorgen dat alle gebruikers met toegang tot een geprivilegieerde account een speciale of secundaire nominatieve account gebruiken voor het uitvoeren ICT activiteiten waarvoor verhoogde rechten nodig zijn. Dit geprivilegieerde account mag alleen worden gebruikt voor deze administratieve activiteiten en niet voor het uitvoeren van de dagdagelijkse operationele activiteiten, surfen op het internet, e-mail of soortgelijke activiteiten.
- alle activiteiten m.b.t. het gebruik en het beheer van deze geprivilegieerde accounts op te nemen in logbestanden en integriteitsbeschermende maatregelen voor deze logbestanden te voorzien.

9) Aanbeveling
De politiezone wordt aangespoord tot het versterken van toezicht en controles teneinde te kunnen beschikken over een correct en actueel inzicht in de werking en effectiviteit van de integrale informatiebeveiliging. Dit houdt onder meer in:

- Het toezien op het naleven van wettelijke, regelgevende en contractuele verplichtingen alsook van de eigen beleidslijnen met betrekking tot informatieveiligheid en in het bijzonder de verwerking van persoonsgegevens;
- Het regelmatig controleren of de informatiesystemen in overeenstemming zijn met de normen voor de tenuitvoerlegging van de beveiliging en het meten van de technische conformiteit kan onder meer door het uitvoeren van *vulnerability scans*, *penetration testing* en *security audit/review*;
- Een periodieke doorlichting uitgevoerd door een onafhankelijke derde partij is een absolute meerwaarde.

10) Aanbeveling
Het is aanbevolen een ICT noodvoorzieningsplan (*DRP* of *Disaster Recovery Plan*) en continuïteitsplan voor alle kritieke processen en essentiële informatiesystemen van de organisatie op te stellen en om dit op periodieke basis te testen. Een *DRP* voor ICT gaat veel verder dan louter een *back-up* voorzien. Het bereid je de organisatie voor op alle mogelijke calamiteiten die de ICT-systemen kunnen ondervinden is de te stellen vraag.

Corrigerende maatregelen,

Gelet op artikel 221 § 1, en 247, 4°,5° en 6°, WGB;

Gelast de politiezone:

a) om de toegang tot de camerabeelden in overeenstemming te brengen met artikel 25/7 § 1, 3e lid, WPA, zodat de reden van de bevragingen geregistreerd wordt. Het bewijs van deze wetsconforme implementatie wordt binnen de negen maanden na datum van kennisname[108] van deze corrigerende maatregel aan het Controleorgaan overlegd;

b) om de logbestanden overeenkomstig artikel 56 WGB bij te houden. Het bewijs van deze wetsconforme implementatie wordt binnen de negen maanden na datum van kennisname van deze corrigerende maatregel aan het Controleorgaan overlegd;

c) de criteria voor opname op deze lokale lijsten te verduidelijken en binnen de drie maanden na kennisname van deze corrigerende maatregel aan het Controleorgaan over te maken;

d) om op regelmatige basis loggings op te vragen van de ANG en proactieve controles door middel van steekproeven (2 x/jaar) te houden met het doel toezicht te houden op het verplicht ingeven van een reden van raadpleging en op eventuele onrechtmatige consultaties en dit een eerste maal binnen de zes maanden na kennisname van deze corrigerende maatregel en de resultaten ervan ter beschikking te houden van het COC.

e) om een informatieveiligheidsplan op te maken. Het informatieveiligheidsplan wordt binnen de negen maanden na datum van kennisname van onderhavig rapport ter beschikking gesteld van het Controleorgaan;

Zegt voor recht dat de aanvangsdatum van de corrigerende maatregelen en de datum van kennisname ervan bedoeld onder de littera a) tot en met e) moet begrepen worden als zijnde de datum van het overmaken van het huidig definitief rapport van het Controleorgaan per e-mail tegen ontvangstbevestiging vermeerderd met twee dagen.

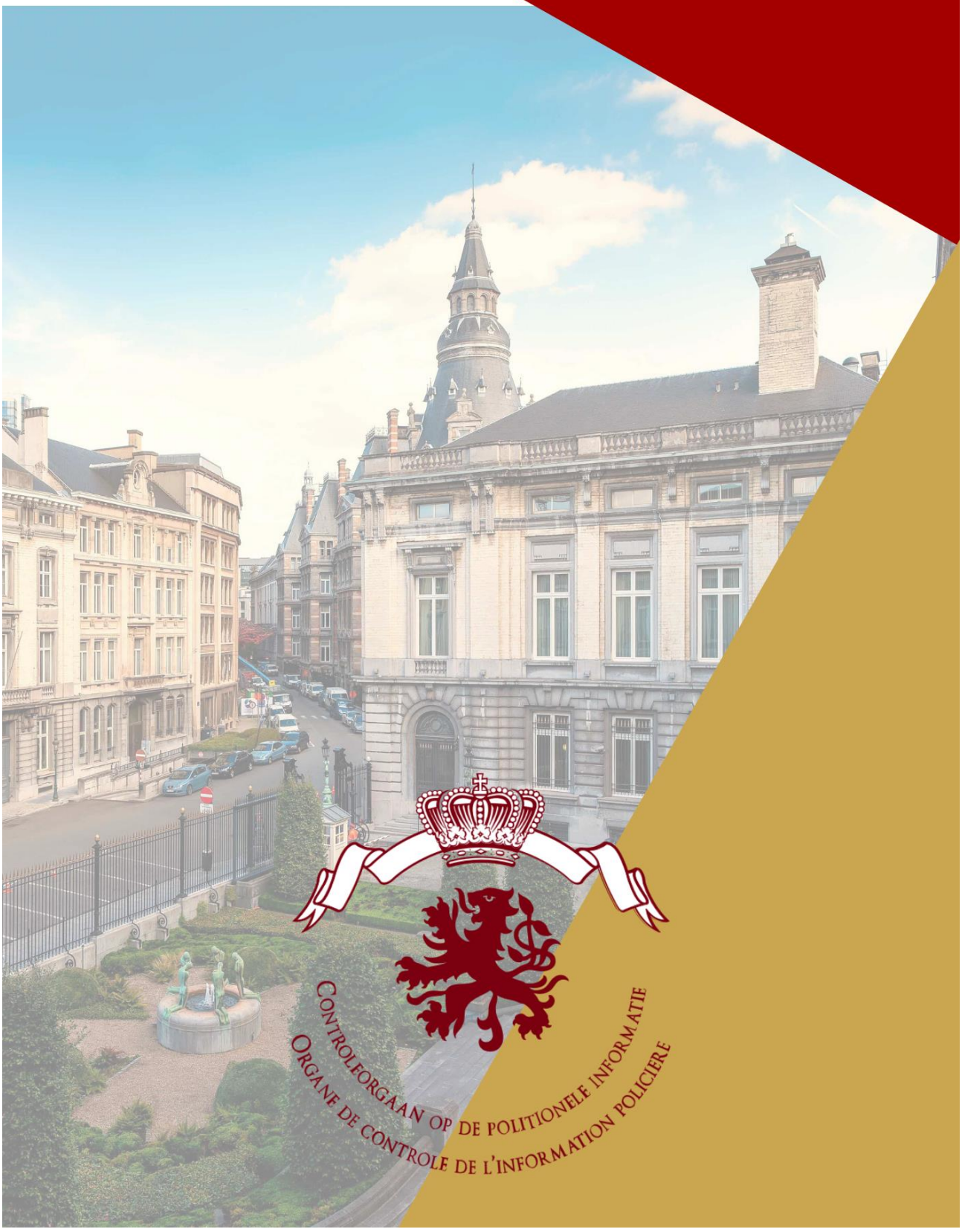
Het Controleorgaan wijst op de mogelijkheid voor de partijen om binnen de dertig dagen na de beslissing van het Controleorgaan beroep aan te tekenen bij het hof van beroep van de woonplaats of zetel van eiser (artikel 248 § 1, 1e lid en § 2 WGB).

Aldus beslist door het Controleorgaan op de Politionele Informatie op 17 februari 2021.

Voor het Controleorgaan

Philippe Arnoud
Voorzitter

[108] Het COC neemt als datum van kennisname de datum van verzending van het rapport vermeerderd met twee werkdagen (indien de vervaldag op een zaterdag, zondag of feestdag valt verschuift de datum van kennisname naar de eerstvolgende werkdag).



Controleorgaan op de politionele informatie

Organe de contrôle de l'information policière