

**PUBLIEKE VERSIE**

**TOEZICHTRAPPORT EN VISITATIE BIJ EEN  
POLITIEZONE IN DE PROVINCIE WEST-  
VLAANDEREN DOOR HET CONTROLEORGAAN OP DE  
POLITIONELE INFORMATIE IN HET KADER VAN  
ZIJN CONTROLE- EN TOEZICHTSBEVOEGDHEDEN**

*Referte: CON20008*

**CONTROLEORGAAN OP DE  
POLITIONELE INFORMATIE**



## PUBLIEKE VERSIE<sup>1</sup>

### 1. INLEIDING

Gelet op zijn bevoegdheden als externe controledienst en bevoegde toezichhoudende autoriteit ten aanzien van de gegevensverwerkingen door de geïntegreerde politie georganiseerd op twee niveaus (GPI) heeft het Controleorgaan op de politionele informatie ('Controleorgaan' of 'COC') beslist een visitatie te verrichten bij politiezone in de provincie West-Vlaanderen (hierna PZ WVL). Onderhavig verslag heeft betrekking op de onderzoeksbevindingen van de visitatie.

#### 1.1. De bevoegdheden van het Controleorgaan op de politionele informatie

De wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (WGB)<sup>2</sup> heeft het Controleorgaan op de politionele informatie hervormd tot onder meer een volwaardige toezichhoudende autoriteit bovenop de bestaande controlerende bevoegdheden inzake politionele informatiehuishouding zoals voorzien in de Wet van 5 augustus 1992 op het Politieambt (WPA). In artikel 71 § 1 en de hoofdstukken II en III van titel 7 WGB worden de opdrachten en de bevoegdheden van het COC omschreven. Daarin 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 toezichhoudende en een controlerende opdracht. Dit betekent dat, naast privacy en gegevensbescherming, het COC ook aandacht heeft voor elementen als efficiëntie en effectiviteit van de informatiehuishouding en het politieoptreden.

Het Controleorgaan is bevoegd voor de politiediensten<sup>3</sup>, de Algemene inspectie van de federale en lokale politie (AIG)<sup>4</sup> en de Passagiersinformatie-eenheid (PIE)<sup>5</sup>. De toezichtbevoegdheid van het Controleorgaan, wat betreft de politiediensten, omvat zowel de operationele als niet-operationele verwerkingsactiviteiten.<sup>6</sup>

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, 3<sup>e</sup> 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.

<sup>1</sup> De publieke versie van een rapport van het Controleorgaan betekent dat deze niet of niet noodzakelijk alle elementen, die vermeld worden in het basisrapport dat aan de bestemmelingen (politie, bestuurlijke en gerechtelijke overheden) wordt gericht, bevat. 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 geredieerd aan een tekortkoming, enz...

<sup>2</sup> 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 (hierna de Richtlijn politie-justitie of LED (*Law Enforcement Directive*)).

<sup>3</sup> Zoals gedefinieerd in artikel 2, 2<sup>o</sup> van de wet van 7 december 1998 tot organisatie van een geïntegreerde politie, gestructureerd op twee niveaus (art. 26, 7<sup>o</sup>, a WGB).

<sup>4</sup> 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<sup>o</sup>, d WGB).

<sup>5</sup> Zoals bedoeld in hoofdstuk 7 van de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens (art. 26, 7<sup>o</sup>, f WGB). Ook wel aangeduid als BELPIU (*Belgian Passenger Information Unit*).

<sup>6</sup> Art. 4 § 2 vierde lid, wet van 3 december 2018 tot oprichting van de Gegevensbeschermingsautoriteit (WOG).

In het kader van het gebruik van niet-zichtbare camera's fungeert het Controleorgaan als een soort "BAM"-commissie<sup>7</sup>. Overeenkomstig 46/6 van de 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<sup>8</sup>. In dat verband beschikken de leden van het Controleorgaan en de leden van de dienst onderzoeken over onderzoeksbevoegdheden en kunnen corrigerende maatregelen worden genomen<sup>9</sup>.

Tegen bepaalde beslissingen van het Controleorgaan staat binnen de dertig dagen een juridische 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<sup>10</sup>.

## 2. OPZET VAN DE VISITATIE EN METHODOLOGIE

Op 26 oktober 2020 heeft het Controleorgaan op eigen initiatief een zgn. beperkte technische visitatie<sup>11</sup> uitgevoerd bij de PZ WV . De visitatie is derhalve 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 politiezone.

Gelet op de omvang, de aard van de gegevens en de vorm van de verwerkingen in het kader van het oprichten van bijzondere gegevensbanken, de gerechtelijke aanhoudingen binnen de politie en de daarbij horende zgn. 'triptiek' gaat het bij dergelijke gegevensverwerkingen om een verregaande inmenging in de persoonlijke levenssfeer. Met het oog op een correcte informatie-inwinning zijn deze verwerkingen gekoppeld aan uitvoeringsvoorwaarden die beschreven worden in de wetgeving (voornamelijk de WPA), uitvoeringsbesluiten en richtlijnen (waaronder voornamelijk de zgn. MFO3). Er wordt door het COC nagegaan of de bijzondere gegevensbanken volgens de toepasselijke regels in het leven geroepen werden, de uitvoering van de gerechtelijke aanhoudingen en triptiek in overeenstemming is met de toepasselijke regelgeving en op een kwalitatieve manier gebeurt.

Met dit soort technische visitaties beoogt het COC een inzicht te verwerven in de werkingsprocessen van de politiezone met betrekking tot de politionele informatiehuishouding. Deze visitatie wordt *in casu* afgebakend tot volgende specifieke thema's:

- bijzondere gegevensbanken;
- 'triptiek'<sup>12</sup> – gerechtelijke aanhoudingen;
- controle op de loggings ANG en reden bevraging;
- stand van zaken/aandachtspunten inzake de 'centrale validatie/optie 35'.

De visitatie valt uiteen in twee fasen.

In de eerste fase werden aan de PZ WV de nodige informatie en stukken opgevraagd. Afhankelijk van de inhoud van de antwoorden en stukken werden specifieke vragen gesteld met het oog op nader onderzoek tijdens de visitatie.

De tweede fase had betrekking op het bezoek ter plaatse (de visitatie), dat als volgt werd opgesplitst:

- 1) een introductie van het COC en de aanwezige leden van de PZ WV;

<sup>7</sup> BAM staat voor 'Bijzondere Administratieve Methoden'.

<sup>8</sup> Art. 240, 4° WGB.

<sup>9</sup> Art. 244 en 247 WGB.

<sup>10</sup> Art. 248 WGB.

<sup>11</sup> Een technische visitatie is een hoofdzakelijk operationeel-politioneel technisch onderzoek met telkens één of meerdere specifieke onderwerpen, zoals de 'controle van de triptiek', 'de ANG-voeding', de 'onrechtmatige toegang/logging' (zie ook artikel 236 §3 en artikel 239 WGB). Dit soort visitatie is minder specifiek gericht op juridische aspecten of aspecten van gegevensbescherming of privacy hoewel deze wel worden meegenomen.

<sup>12</sup> De triptiek betreft het afnemen van vinger- en handpalmafdrucken, het nemen van foto's en het opstellen van de individuele beschrijving om tot een identificatie van een persoon te komen (zie ook randnummer 13).

- 2) bespreking van de ons toegestuurde documenten met betrekking tot de bijzondere gegevensbanken van de PZ WV;
- 3) een bezoek aan het 'FIT-station'<sup>13</sup>
- 4) een bezoek aan het functioneel beheer
- 5) een algemene rondleiding in het commissariaat met *ad hoc* vragen die konden gesteld worden.

## 3. Juridisch kader

### 3.1. Bijzondere gegevensbanken (GBO)

Artikel 44/11/3 §1 WPA voorziet als voorwaarde voor de oprichting van een GBO dat dit enkel mogelijk is onder de volgende cumulatieve voorwaarden:

- in specifieke omstandigheden;
- voor de uitoefening van de opdrachten van bestuurlijke of gerechtelijke politie;
- voor bijzondere behoeften.

Artikel 44/11/3 §2 WPA voorziet verder dat de oprichting van een GBO (bijkomend) door minstens één van de volgende bijzondere behoeften moet worden verantwoord:

- a) de noodzaak om persoonsgegevens en informatie te classificeren in de zin van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen;
- b) de technische of functionele onmogelijkheid om de ANG te voeden met alle of een gedeelte van de in deze gegevensbanken verwerkte persoonsgegevens en informatie;
- c) het niet ter zake dienend of overmatig karakter van de centralisering van alle of een gedeelte van de persoonsgegevens of de informatie in de ANG in het kader van de uitoefening van de opdrachten van bestuurlijke politie en van gerechtelijke politie.

Conform art. 58 en 59 van de WGB zullen de politiediensten vooraf het advies van het COC moeten vragen wanneer:

- de verwerking, in het bijzonder bij gebruik van nieuwe technologieën, een hoog risico oplevert voor de rechten en vrijheden van natuurlijke personen (art. 58);
- uit de DPIA<sup>14</sup> een hoog risico blijkt en de verwerkingsverantwoordelijke niet de nodige maatregelen neemt om het risico te beperken; of indien de aard van de verwerking, in bijzonder bij gebruik van nieuwe technologieën, mechanismen of procedures, een hoog risico voor de rechten en vrijheden van de betrokkenen met zich brengt (art. 59 §1 1° en 2°).

De GPI kan dus bijvoorbeeld niet de volgende argumenten weerhouden om een bijzondere gegevensbank op te richten:

- werklast vereist voor de vatting, de voeding en de overdracht van de gegevens naar de ANG;
- gebrek aan kennis van het gebruik van een ANG of een basisgegevensbank;
- gebrek aan (beweerdelijke) gebruiksvriendelijkheid van de ANG of een basisgegevensbank.

### 3.2. Triptiek

Het uitvoeren van de triptiek is essentieel in de doelstelling om de juiste informatie op het juiste ogenblik op de juiste plaats te brengen met het oog op een efficiëntere en effectievere uitvoering van de opdrachten van gerechtelijke en bestuurlijke politie.

De gerechtelijke triptiek wordt uitgevoerd om bij te dragen tot de identificatie van personen en bestaat uit 3 luiken:

- a: vinger- en handpalmafdrukken;

<sup>13</sup> FIT-station staat voor *Fingerprint Image Transmission*.

<sup>14</sup> DPIA staat voor *Data Protection Impact Assessment*.

- b: foto's;
- c: individuele persoonsbeschrijving.

### 3.4. Logging ANG

De politie is verplicht om logbestanden bij te houden<sup>15</sup>. 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 garanderen<sup>16</sup>. In dat verband zijn logbestanden tevens van belang bij interne tuchtprocedures of administratieve onderzoeken. Cijfers van de tuchtraad van de GPI tonen aan dat een onrechtmatige raadpleging het meest frequent gepleegde tuchtmisdrijf is. Logbestanden zijn bijgevolg van belang met het oog op zowel proactieve als reactieve controle en zowel op intern als op extern niveau.

## 4. ONDERZOEKSBEVINDINGEN

### 4.1. Bijzondere gegevensbanken

Voorafgaand aan de visitatie werd een beleidsdocument m.b.t. de oprichting en het gebruik van bijzondere gegevensbanken door het Controleorgaan ontvangen. Het COC stelde vast dat de PZ WVl pas na de aankondiging van de visitatie door het COC dit beleidsdocument heeft opgemaakt. Uit de lezing blijkt dat wat vervat zit voldoet aan wat als wettelijk kader in de WPA vermeld wordt, evenals de aanzet vormt om een actieplan op touw te zetten om de bijzondere gegevensbanken te evalueren en te implementeren. **Dit beleidsdocument kan dus beschouwd worden als een eerste en goede stap in het proces om tot een eenduidig beleid in het kader van de implementatie van de bijzondere gegevensbanken in de politiezone te komen.**

De in de bijlage bij voormeld beleidsdocument opgenomen bijzondere gegevensbanken werden volgens de PZ reeds 10 à 15 jaar geleden in gebruik genomen. Dit brengt met zich dat men al deze bijzondere gegevensbanken, volgens het stappenplan voorzien in het document, zal moeten overlopen om na te gaan of deze al dan niet voldoen aan de wettelijke bepalingen. Deze oefening zal volgens de PZ WVl gemaakt worden door de informatieveiligheidscel (IVC) die is samengesteld uit sleutelfiguren met de nodige competenties binnen de PZ. Na de eerste evaluatie zullen de weerhouden bijzondere gegevensbanken, evenals nieuwe op te richten bijzondere gegevensbanken, aan een trimestriële evaluatie door de IVC onderworpen worden.

Uit het beleidsdocument blijkt verder dat, indien een bijzondere gegevensbank weerhouden wordt, deze door de *Data Protection Officer (DPO)* zal geregistreerd worden in het REGPOL<sup>17</sup>. Het feit dat er nog geen uitvoeringsbesluit is verschenen om de gegevens verplicht in het REGPOL aan te geven ontslaat de PZ namelijk niet van de verplichting om de gegevensbanken in een eigen register der verwerkingen bij te houden. **De PZ gaf sowieso aan de intentie te hebben om de gegevensbanken in het REGPOL aan te geven; er bleek dan ook geen eigen register voorhanden.** Bijgevolg is er tot op datum van 22/10/20 nog geen bijzondere gegevensbank geregistreerd, noch werden deze in het verleden bij het COC aangemeld zoals nochtans reeds verplichtend was gesteld door het oude artikel 44/11/3 §3<sup>18</sup>.

**Ondanks het feit dat de evaluatie van de reeds in het korps gebruikte bijzondere gegevensbanken nog dient te gebeuren is de korpsleiding zich er van bewust dat de politiezone niet voldoet aan de regels inzake actualisering van de gegevens, het bewaren en wissen ervan, enz. ...**

Evenals het COC is de PZ er ook voorstander van om in het kader van een goede gegevensuitwisseling zoveel als mogelijk de basisgegevensbanken te voeden en enkel met in achtneming van in de wet vastgelegde criteria gebruik te maken van een GBO.

<sup>15</sup> Art. 56 § 1, WGB, ter uitvoering van artikel 25 Richtlijn Politie & Justitie.

<sup>16</sup> Art. 56 § 2, WGB.

<sup>17</sup> REGPOL is het nationaal register van de persoonsgegevensverwerkingen zoals opgenomen in art. 145, 2<sup>e</sup> lid Wet Geïntegreerde Politie van 7 december 1998 (dit register ICT technisch ondersteund door de federale politie).

<sup>18</sup> Zoals dat van toepassing was tot 29 juni 2019, datum van inwerkingtreding van de Wet van 22 mei 2019 tot wijziging van diverse bepalingen wat het politiebureau informatiebeheer betreft die deze aanmelding heeft opgeheven door een wijziging van onder meer deze paragraaf 3 (cf. artikel 14).

Op basis van wat er tijdens de visitatie werd meegedeeld komt het COC tot de onderstaande vaststellingen voor de opgesomde bijzondere gegevensbanken:

- er is slechts één applicatiebeheerder die instaat voor de opmaak van de bijzondere gegevensbanken;
- van de bestaande gegevensbanken konden geen 'stroomdiagrammen, die de *workflows* binnen de bijzondere gegevensbanken in kaart brengen, voorgelegd worden. De functionele analyses worden *on te spot* gemaakt in samenspraak met diegene die nood heeft of beweerd nood te hebben aan een bijzondere gegevensbank, maar worden verder nergens gedocumenteerd. Op basis van dergelijke stroomdiagrammen kan uitgemaakt worden of de gegevens gevat in een bijzondere gegevensbank niet beter gevat kunnen worden in bv. een basisgegevensbank;
- **voor geen enkel van de gegevensbanken werden termijnen voor evaluatie van de bewaarde gegevens voorzien;**
- **de gegevensbanken kunnen bevroegd worden zonder dat er een reden van raadpleging vermeld dient te worden.**

**Nochtans is het voorzien van regelmatige evaluatiemomenten een goede praktijk en blijkt de verplichting tot het vermelden van een reden voor raadpleging uit de artikelen 56 §1, 2 en 3 WGB *juncto* 44/11/3 §4 WPA.**

De PZ WWL vermeldt in het beleidsdocument dat er per bijzondere gegevensbank een logging voor de verwerkingen moet worden voorzien. Het korps zal eveneens in specifieke profielen voorzien om de logbestanden te gebruiken. Zo wordt belang gehecht aan het trekken van de juiste conclusies uit de loggingsresultaten. De PZ stelt dat voor de desbetreffende bijzondere gegevensbanken loggingsgegevens beschikbaar zijn of op vraag van het COC kunnen worden voorzien. Deze loggings zijn momenteel enkel toegankelijk voor specifieke profielen binnen de PZ.

## 4.2. Triptiek

Naar aanleiding van de visitatie werd op voorhand een lijst van gerechtelijke aanhoudingen van de PZ WWL opgevraagd. Uit deze lijst werden willekeurig vijf gerechtelijke aanhoudingen weerhouden om na te gaan of de triptiek conform de richtlijnen en kwalitatief werd uitgevoerd.

Verder werd de invoer van de benodigde gegevens in ISLP gecheckt van waaruit kon nagegaan worden of de flux van ISLP<sup>19</sup> naar de ANG<sup>20</sup> correct verlopen was en de personen correct werden gevat.

Uit deze beperkte steekproef bleek dat de triptiek in de PZ onvoldoende wordt afgenomen. Waar de richtlijnen duidelijk zijn dat bij elke gerechtelijke aanhouding een triptiek dient afgenomen te worden is gebleken dat **in vier van de vijf gevallen de triptiek niet of niet volledig werd uitgevoerd**. In één geval was de triptiek wel volledig en daar kon het AFIS-nummer<sup>21</sup> ook worden teruggevonden in de basisgegevensbank ISLP. Deze steekproef lijkt aan te geven dat de uitvoering van de triptiek ruimschoots onvoldoende is en er actie moet worden genomen om dit te corrigeren. Kwaliteitsvolle politionele informatiehuishouding staat of valt met de correcte uitvoering van een reeks van basishandelingen, waaronder de triptiek.

Voor wat de registratie in ISLP betreft van de natuurlijke personen die het voorwerp uitmaken van een gerechtelijke aanhouding kan het COC vaststellen dat vier van de vijf gevallen kunnen teruggevonden met een correcte basis van registratie. Volgens de PZ is het niet terugvinden van één betrokkene in het ISLP-systeem van de PZ WWL het gevolg van de vrijheidsberoving van verdachten door een andere zone of dienst.

De PZ had ondertussen eenzelfde oefening gemaakt voor een lijst van 50 van hun vrijheid beroofde personen. Hieruit bleek **dat in de helft van de gevallen de triptiek niet of niet volledig werd uitgevoerd. Het COC kan hier dus, zoals gezegd, niet anders dan vaststellen dat de wettelijke taak tot het uitvoeren van de triptiek, niet of niet goed uitgevoerd werd conform de geldende richtlijnen**. Hierdoor komt de gegevensuitwisseling naar de algemene nationale gegevensbank (ANG) in het gedrang en daardoor ook een efficiënte en effectieve gegevensverwerking door en voor de hele geïntegreerde politie.

<sup>19</sup> Basisgegevensbank zoals vastgesteld in art. 44/11/2 WPA

<sup>20</sup> Algemene nationale gegevensbank zoals bepaald in art. 44/7 WPA

<sup>21</sup> Identiek nr. in ISLP dat refereert naar de genomen vingerafdrukken

### 4.3. Logging en reden bevraging (ANG-toepassingen)

Het volgende onderzoeksitem in deze technische controle betreft de logging op opvragingen binnen de ANG uitgevoerd door de PZ WVW waarin dan ook de reden van bevraging kan nagegaan worden. De politiemedewerkers kunnen op een aantal manieren operationele informatie opvragen in de ANG om hun werk op een effectieve en efficiënte uit te voeren.

De politie is verplicht om logbestanden bij te houden<sup>22</sup>. 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 garanderen<sup>23</sup>.

De PZ zelf heeft tot op dag van de visitatie geen loggings opgevraagd. **Er gebeurden ook geen proactieve controles op eventuele onrechtmatige consultaties.**

Het COC stelde vast dat er zo goed als geen reden van raadpleging werd ingegeven en, indien dit wel gebeurde, de reden onvoldoende duidelijk was. Indien mogelijk moet steeds een zo concreet mogelijke referentie ingegeven worden bij een reden raadpleging.

### 4.4. Centrale validatie

Een laatste item dat werd onderzocht betrof het uitvoeren van de zgn. centrale validatie<sup>24</sup> binnen de politiezone.

Volgens de PZ wordt deze centrale validatie dagelijks uitgevoerd.

### 4.5. Aanvullende vaststellingen

Niettegenstaande de visitatie een beperkte technische visitatie was stelden we daarnaast tijdens onze rondleiding in het hoofdkantoor van de politiezone enkele zaken vast die opvolging noodzakelijk maken. Dit kan mogelijks deel uitmaken van een bijkomend onderzoek en/of opvolging.

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

Het COC stelde vast dat er aan bepaalde toegangen registratietoestellen hingen die gebruikt worden om, via biometrie (vingerafdrukken), toegang tot lokalen te verlenen en/of in te staan voor tijdsregistratie.

Bij navraag bleek dat de PZ gebruik maakt van biometrische gegevens om toegang te krijgen tot bepaalde lokalen. De biometrische gegevens worden niet gebruikt voor tijdsregistratie. Het COC verstrekte toelichting over de reden waarom het van oordeel is dat het gebruik van biometrische gegevens niet toelaatbaar is. 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 voor het invoeren van het controlesysteem betreft het aspect van authenticatie, met name dat degene die zich toegang verschaft wel degelijk de persoon is met wie de identificatiegegevens overeenstemmen. Bij wijze van alternatief kan gebruik worden gemaakt van de persoonlijk badge.

**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.**

Het COC wijst er op dat er geen enkele wettelijke grondslag voorhanden is tot het gebruik van biometrie als middel tot toegangsbeheer en/of tijdsregistratie (of eender welke andere AVG-toepassing). **Noch de toestemming van de betrokkene noch het zwaarwegend algemeen belang kunnen in aanmerking komen.**

<sup>22</sup> Art. 56 § 1, WGB, ter uitvoering van artikel 25 Richtlijn Politie & Justitie.

<sup>23</sup> Art. 56 § 2, WGB.

<sup>24</sup> De gestructureerde geregistreerde gegevens worden na voorbereiding in de lokale toepassing (ISLP, Lokale vattig, Feedis, ...) overgemaakt aan het centrale niveau, waar ze automatisch gecontroleerd worden.

## 4.5.2. Cameragebruik

Er werd daarnaast ook vastgesteld dat er in de dispatching ruimte van de PZ een grote *videowall* aanwezig was waaruit blijkt dat de PZ over een uitgebreid cameranetwerk beschikt.

Op het gebruik van camerabewaking door politiediensten is door de wet van 21 maart 2018<sup>25</sup> sinds 25 mei 2018 de WPA van toepassing. 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 de wetswijzigingen. Wanneer de politie gebruik maakt van camerabewaking zijn dus de bepalingen van de WPA van toepassing, behalve wanneer het gebruik van camera's in andere wetgeving wordt geregeld. Vooraleer een politiedienst camerabewaking op het grondgebied van gemeente wenst in te voeren, heeft zij daartoe de principiële toestemming van de gemeenteraad nodig<sup>26</sup>. 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<sup>27</sup>. Het is van belang er op te wijzen dat wanneer de toestemming van de gemeenteraad reeds vóór de wetwijziging van 21 maart 2018 werd verkregen onder de toepassing van de (oude) camerawet de toestemming niet opnieuw van de gemeenteraad verkregen moet worden<sup>28</sup>. Deze 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<sup>29</sup>. In dat geval moet dus een nieuwe, of aanvullende, toestemming van de gemeenteraad verkregen worden.

Het COC stelde vast dat de PZ WWL geen toestemming van de gemeenteraad voor het gebruik van camera's kon voorleggen. Bijgevolg voldoet het gebruik van de camera's actueel niet aan alle wettelijke voorwaarden. In haar antwoord op het ontwerp van rapport liet de PZ WWL weten dat "*begin november het nodige werd gedaan om dit op de gemeenteraden te krijgen. Het item kwam aan bod op het politiecollege van midden oktober. Intussen werden reeds 3 toestemmingen ontvangen, en staat het item gepland op de eerstkomende gemeenteraden van de steden en gemeenten waarvoor we nog geen toestemming ontvingen*".

Het COC benadrukt dat **vóór** de ingebruikname van camera's moet voldaan worden aan de wettelijke voorwaarden zoals het hebben van gemeenteraadsbesluiten, *DPIA's*, aangifte REGPOL, enz. ... Vooral de geïnformeerde toestemming van de gemeenteraden die gepaard moet gaan met een *DPIA*<sup>30</sup>, zeker vanuit grondrechtenperspectief, essentieel omdat het de uiting is van de lokale democratische besluitvorming en dito draagvlak.

## 5. CONCLUSIE – VERZOEKEN, AANBEVELINGEN EN CORRIGERENDE MAATREGELEN

De PZ is na de aankondiging van de visitatie begonnen met het schrijven van de tijdelijke korpsnota inzake de bijzondere gegevensbanken. De korpsnota geeft correct weer wat wettelijk bepaald wordt voor wat betreft het in het leven roepen van een bijzondere gegevensbank. Het COC beoordeelt dit als een goede start om op verder te bouwen; het is bijkomend wel hoogdringend de nodige stappen te zetten in het kader van informatieveiligheid en gegevensbescherming.

Informatieveiligheid vergt een continue inzet waarbij een structurele aanpak en periodieke opvolging aangewezen zijn. Het raamwerk informatieveiligheid dient dan ook verder ontwikkeld en geïmplementeerd te worden waarbij op korte termijn een aantal werkzaamheden op gebied van informatieveiligheid verdere opvolging vereisen zoals de implementering van de korpsnota, het sensibiliseren in het kader van de opzoeken en redenen van bevraging, het uitvoeren van de triptiek enz. ... Een adequate aansturing van de verdere implementatie van informatiebeveiliging in

<sup>25</sup> 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.

<sup>26</sup> Art. 25/4 § 1, 1<sup>o</sup> WPA.

<sup>27</sup> Memorie van Toelichting bij deze wet, p. 21 (Parl. St? *kamer* 2017-2018, nr. 54-2588/001).

<sup>28</sup> Art. 88 wet van 21 maart 2018 en Memorie van Toelichting bij deze wet, p. 113-114 (Parl. *Kamer* 2017-2018, nr. 54-2588/001).

<sup>29</sup> Art. 25/4 § 2, 2<sup>de</sup> lid WPA.

<sup>30</sup> Waarin ook de impact – en risicoanalyse op het vlak van de bescherming van de persoonlijke levenssfeer en op operationeel niveau moet vervat zitten, met name wat de categorieën van verwerkte persoonsgegevens betreft, de proportionaliteit van de aangewende middelen, de te bereiken operationele doelstellingen en de bewaartermijn van de gegevens die nodig is om deze doelstellingen te bereiken (art. 25/4 §2, 2<sup>e</sup> lid WPA).



het algemeen binnen de PZ via de informatieveiligheidscel (IVC) is hierbij van primordiaal belang. De *DPO* is één van de sleutelfiguren binnen deze IVC.

Het Controleorgaan is van oordeel dat, ondanks de vaststelling dat er nog een aantal domeinen, ook binnen de scope van dit onderzoek, voor heel wat verbetering vatbaar is, het de PZ niet ontbreekt aan goede wil om deze items aan te pakken en tot een gedegen informatieveiligheidsbeleid te komen en te implementeren. Ook bij de medewerkers die deelnamen aan de visitatie heeft het COC de kennelijke wil vastgesteld om hun taken naar behoren uit te voeren.

**Het Controleorgaan;**

**verzoekt de PZ WV,**

## 1) Verzoek

om een nieuwe algemene stand van zaken m.b.t. de bijzondere gegevensbanken over te maken binnen een termijn van uiterlijk 4 maanden na ontvangst van dit rapport;

**brengt de volgende aanbevelingen uit,**

## 2) Aanbeveling

het COC beveelt aan dat de IVC regelmatig samenkomt om de nodige evaluaties en opvolging met betrekking tot de bijzondere gegevensbanken te kunnen uitvoeren. Gegevens mogen enkel verwerkt worden indien ze nog toereikend, ter zake dienend en niet overmatig zijn. Het COC beveelt aan dat voor de bijzondere gegevensbanken voorzien wordt in een regelmatige evaluatie en het instellen van maximale bewaartermijnen waar mogelijk;

## 3) Aanbeveling

in het kader van een stringent toegangscontrolebeleid m.b.t. de bijzondere gegevensbanken dringt het COC er op aan om gebruik te maken van MFA indien deze technische mogelijkheid kan worden voorzien. Op die manier vermindert men de risico's die inherent zijn aan het gebruik van wachtwoorden;

## 4) Aanbeveling

het Controleorgaan dringt er bij de PZ 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. 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 kwaadwillige geprivilegieerde gebruiker, omwille van hun uitgebreide toegangsrechten, in principe de sporen van zijn activiteiten wissen door bijvoorbeeld de systeemlogbestanden aan te passen of deze geheel te wissen;

## 5) Aanbeveling

conform art. 28, 6° van de Wet Gegevensbescherming moet voorzien worden in passende technische of organisatorische maatregelen zodat dat de beveiliging van de bijzondere gegevensbanken gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging. Het COC beveelt aan om de bijzondere gegevensbanken aan te maken volgens een geijkte procedure met nadruk op de technische fiche om te voldoen aan de gevraagde veiligheidseisen van art. 28, 6° WGB;

## 6) Aanbeveling

conform de ministeriële richtlijn MFO-3 moet steeds overgegaan tot het uitvoeren van de volledige of gedeeltelijke triptiek die daarin werd vastgelegd. In het raam van de grote tekortkoming vastgesteld in het uitvoeren van de triptiek in de PZ dringt het COC er op aan om deze richtlijnen te communiceren, te duiden en regelmatig te herhalen (door middel van bewustmakingscampagnes). Het is tevens van belang om blijvend via diverse informatiekanaal (mails/intranet/informatiesessies/vormingen/...) te voorzien in structurele en periodieke voorlichting rond het uitvoeren van de triptiek;

## 7) Aanbeveling

hoewel het Controleorgaan vaststelt dat er op regelmatige basis in de centrale validatie gewerkt wordt is het wenselijk om deze niet te hoog te laten oplopen. Het aantal verwerpingen onder 100 regels houden dient een na te streven doel te zijn. Het COC beveelt aan om te voorzien in een *back-up* van de medewerk(st)er die de verwerpingen behandelt;

## **Gelest de volgende corrigerende maatregelen ten aanzien van de PZ WV,**

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

8.a) een functionele analyse te maken van de bijzondere gegevensbanken. De bijzondere gegevensbanken die niet meer voldoen aan de wettelijke bepalingen dienen geschrapt te worden en de gegevens gewist te worden. Zolang deze analyse niet voltooid werd en gezien de bijzondere gegevensbanken nu operationeel in gebruik zijn bestaat er een reëel risico van het onrechtmatig verwerken van persoonsgegevens. Deze analyse zal aan het COC overgemaakt worden binnen een termijn van 6 maanden na ontvangst van deze corrigerende maatregel;

8.b) aangifte te doen van de bijzondere gegevensbanken en de in de politiezone gebruikte camera's bij voorkeur in REGPOL, subsidiair minstens bij te houden in een eigen register van verwerkingen en het Controleorgaan daarvan de bevestiging en het overzicht te laten geworden binnen een termijn van 6 maanden na kennisname van deze corrigerende maatregel;

8.c) voor het raadplegen van de bijzondere gegevensbanken te voorzien in een invulveld dat moet toelaten de reden raadpleging te noteren. Het gebruik van een aanvinkvakje is niet voldoende om tot een identificeerbaar gegeven te komen en te voldoen aan de wettelijke bepalingen van de artikelen 56 §1, 2 en 3 WGB *juncto* 44/11/3 §4 WPA. Het Controleorgaan legt de termijn van uitvoering vast op 6 maanden vanaf de datum van kennisname van deze corrigerende maatregel;

8.d) een *policy*/beleid op te stellen dat voorziet in een mechanisme waardoor periodiek en effectief controles worden uitgevoerd op het monitoren van eventuele (on)rechtmatige consultaties van de bijzondere gegevensbanken. De logbestanden van de verwerkingen moeten bewaard worden gedurende minimum tien jaar. De verwerkingsverantwoordelijke kan, indien nodig, bij een gemotiveerde beslissing en na evaluatie deze termijn verlengen met een maximale periode van twintig jaar. Het COC verzoekt om te voorzien in de nodige logbestanden die op een eenvoudige manier ter beschikking of ter inzage kunnen worden gesteld van de betreffende toezichtsorganen. Het Controleorgaan beveelt een verplichte tweemaalige jaarlijkse controle van de loggings door de PZ en de resultaten ter beschikking te houden van COC;

8.e) 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;

8.f) in de loop van 2021 of uiterlijk binnen een termijn van één jaar na kennisname van deze corrigerende maatregel geen gebruik meer te maken van de biometrische toegangscontrole en na afloop van voormelde termijn er zorg voor te dragen dat enkel nog een alternatief systeem van toepassing zal zijn zonder een verwerking van biometrische gegevens;

9) er zorg voor te dragen dat, voor het gebruik van de verschillende soorten camera's waaronder de bewakingscamera's en de vaste en mobiele *ANPR's*, de wettelijk voorziene gemeenteraadsbesluiten, gepaard gaande met de in artikel 25/4

## RAPPORT

§2, 2<sup>e</sup> lid WPA vermelde impact- en risicoanalyse en de nodige *DPIA's*, werden genomen en het COC op de hoogte te stellen van zodra alle gemeenteraadsbesluiten werden genomen en dit binnen de vier maanden na kennisname van deze corrigerende maatregel

Zegt voor recht dat de aanvangsdata van de corrigerende maatregelen en de datum van kennisname ervan bedoeld onder de littera 8.a) tot en met f) en 9 moet begrepen worden als zijnde de datum van het overmaken van het huidig definitief rapport van het Controleorgaan vermeerderd met twee dagen.

Het Controleorgaan wijst op de mogelijkheid voor de politiezone om binnen de 30 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).

Aldus beslist door het Controleorgaan op de Politiezone Informatie op 12 januari 2021.

Voor het Controleorgaan,

Philippe Arnoud  
Voorzitter