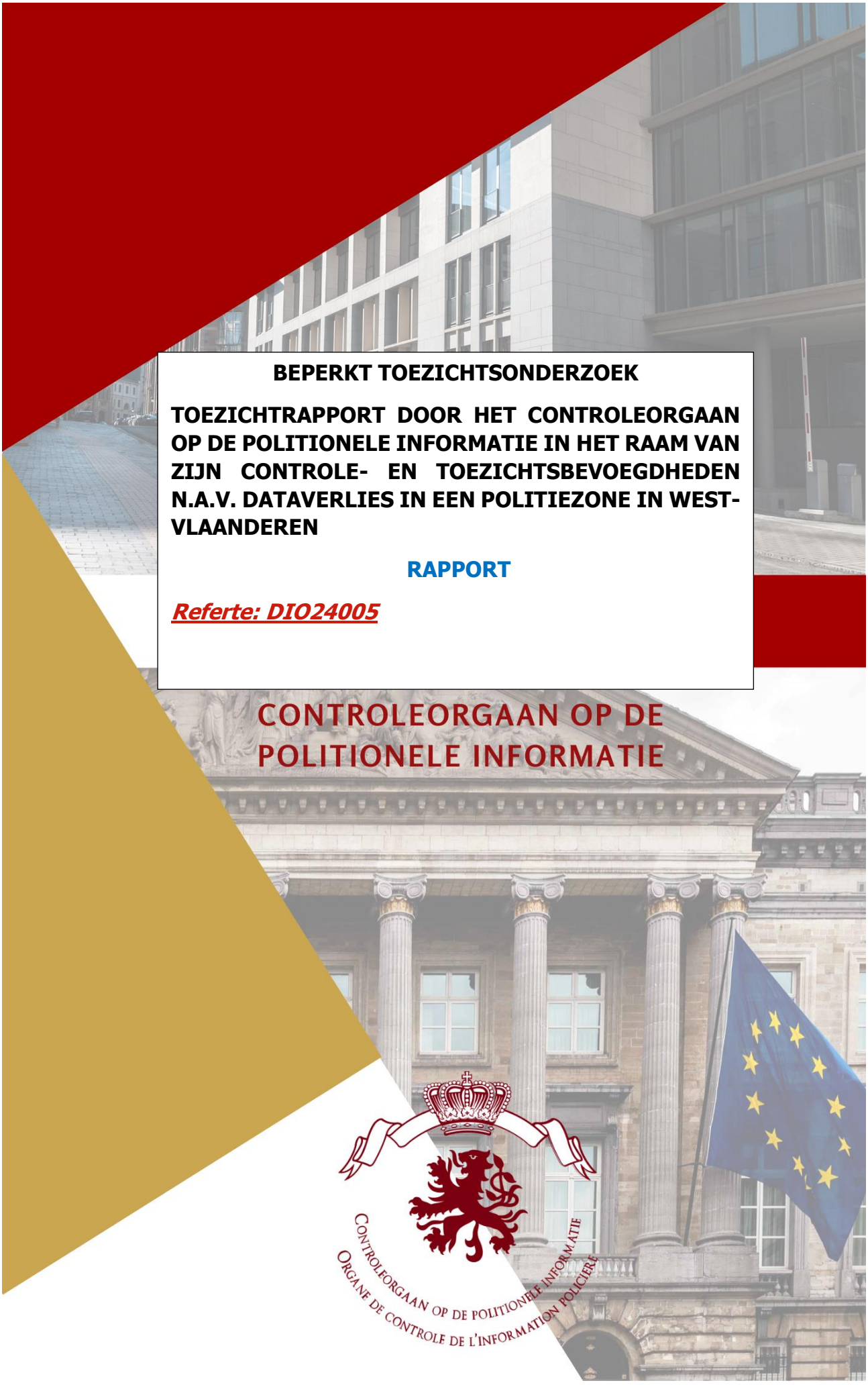


BEPERKT TOEZICHTSONDERZOEK

TOEZICHTRAPPORT DOOR HET CONTROLEORGAAN OP DE POLITIONELE INFORMATIE IN HET RAAM VAN ZIJN CONTROLE- EN TOEZICHTSBEVOEGDHEDEN N.A.V. DATAVERLIES IN EEN POLITIEZONE IN WEST-VLAANDEREN

RAPPORT

Referte: DIO24005

1. Inhoud

1. RAPPORT

Dit rapport betreft een **publieke versie** van het toezichtonderzoek.

Dit betekent dat het niet of niet noodzakelijk alle elementen of passages bevat die vermeld worden in het basisrapport dat 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 een tekortkoming inmiddels werd verholpen, enz. …

2. INLEIDING

Abstract

Op 12 november 2023 werd het COC in kennis gesteld van een verlies aan data op 31 oktober 2023 bij een Politiezone in West-Vlaanderen (PZ WVL). Het ging hierbij om een menselijke fout waarbij alle digitale inbeslagnames van 2022 verloren zijn gegaan. Er bleek geen back-up te zijn niettegenstaande dit volgens diverse richtlijnen en aanbevelingen vereist is. Dit rapport bekijkt de verplichtingen rond back-up in het kader van wetgeving, richtlijnen, aanbevelingen.

Bijkomend worden er vragen gesteld naar de antwoordtermijnen die de PZ WVL hanteert evenals het verwijderen en het onherkenbaar maken van elementen in de documenten die aan het COC overgemaakt worden. Het rapport eindigt met enkele aanbevelingen.

Keywords

Politiezone West-Vlaanderen, informatieveiligheid - back-up, digitale inbeslagname, ISO 27k, high-availability, redundantie

3. DE BEVOEGDHEDEN VAN HET CONTROLEORGAAN OP DE POLITIONELE INFORMATIE

1. De wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (WVG of Wet Gegevensbescherming)[1] heeft het Controleorgaan 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 (WPA). In artikel 71 § 1 en de titels 2 en 7 WVG 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 44/11/14 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 de informatiehuishouding en het politieoptreden. Het COC heeft op grond van bovenstaande regelgeving derhalve een algemene toezichtsbevoegdheid op alle operationele en niet operationele (persoons)gegevensverwerkingen door de GPI.

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.

[1] *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* (***L**aw **E**nforcement **D**irective*)).

1. RAPPORT

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 de artikelen 44/1 tot 44/11/14 WPA en met hun uitvoeringsmaatregelen.

In het raam van het gebruik van niet-zichtbare camera's fungeert het Controleorgaan als een soort "BAM"-commissie[2]. 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[3]. De leden en de personeelsleden van het Controleorgaan[4] beschikken over onderzoeksbevoegdheden en vervolgens kunnen, naast verzoeken en aanbevelingen, door het directiecomité van het COC ook corrigerende maatregelen worden genomen[5], deze laatsten als *ultimum remedium* wanneer inbreuken worden vastgesteld op de toepasselijke regelgeving.

Het Controleorgaan is, ten aanzien van de politiediensten, de Algemene Inspectie van de federale politie en lokale politie (afgekort 'AIG') zoals bedoeld in de wet van 15 mei 2007 "*op de Algemene Inspectie en houdende diverse bepalingen betreffende de rechtspositie van sommige leden van de politiediensten*" en de Passagiersinformatie-eenheid (hierna afgekort 'BELPIE') bedoeld in Hoofdstuk 7 van de wet van 25 december 2016 "*betreffende de verwerking van passagiersgegevens*" tevens belast met het toezicht op de toepassing van Titel 2 van de WVG en/of de verwerking van persoonsgegevens zoals bedoeld in de artikelen 44/1 tot 44/11/14 van de wet op het politieambt en/of elke andere opdracht die haar krachtens of door andere wetten wordt verleend[6].

Het Controleorgaan is ingevolge artikel 281, § 4, van de algemene wet van 18 juli 1977 "*inzake douane en accijnzen*", zoals gewijzigd door de wet van 2 mei 2019 "*tot wijziging van diverse bepalingen met betrekking tot de verwerking van persoonsgegevens*" ten aanzien van de Dienst Geschillen van de Algemene Administratie van Douane en Accijnzen bevoegd in het kader van de vorderingen gericht aan de BELPIE in fiscale materies.

Het COC is tot slot ook belast, in het kader van de dataretentie wetgeving, op grond van artikel 126/3 §1, 8e lid van de wet van 13 juni 2005 betreffende de elektronische communicatie (hierna afgekort 'WEC')[7], met de (al dan niet) validatie van de statistieken met betrekking tot het aantal strafbare feiten en de bewaringstermijn voor elk gerechtelijk arrondissement en elke politiezone in het kader waarvan het al zijn bevoegdheden uitoefent die hem zijn toegekend in titel 7 WVG. Het is daarnaast ook nog belast, in toepassing van artikel 42 § 3, 2de en 3de lid WPA met de controle van de vorderingen van de Cel Vermiste Personen van de federale politie tot opvraging van de gegevens met betrekking tot de elektronische communicatie betreffende de vermiste persoon.

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[8].

4. OPZET VAN HET TOEZICHT EN METHODOLOGIE

2. Op 12 november 2023 werd het COC door een politiezone in West-Vlaanderen (PZ WVL) op de hoogte gebracht[9] van een zgn. *data breach* (melding inbreuk op de beveiliging[10]), zoals geregeld in artikel 61 WVG. Op basis van de elementen

[2] BAM staat voor '**B**ijzondere **A**dministratieve **M**ethoden'.
[3] Art. 240, 4° WVG.
[4] Met name de personeelsleden van de **D**ienst **O**nderzoeken / **S**ervice d'Enquête (DOSE) en het secretariaat, zijnde juristen en ICT-deskundigen.
[5] Art. 244 (onderzoeksbevoegdheden voor leden en personeelsleden) en 247 WVG (corrigerende maatregelen te nemen door het directiecomité (DIRCOM) van het COC).
[6] Artikel 71 §1, derde lid juncto 236 § 3 WVG.
[7] Zoals gewijzigd door de wet van 20 juli 2022 betreffende het verzamelen en het bewaren van de identificatiegegevens en van metagegevens in de sector van de elektronische communicatie en de verstrekking ervan aan de autoriteiten (*BS* van 8 augustus 2022).
[8] Art. 248 WVG.
[9] COC Dossier DB230034.
[10] "*"inbreuk op de beveiliging": een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde bekendmaking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens*" (art. 26, 11° WVG).

in dit dossier heeft het COC besloten een beperkt toezicht op te starten waarvan de resultaten in dit rapport worden opgenomen.

3. Uit het antwoord van de PZ WVL aangaande de vaststelling dat er géén *back-up* wordt genomen van het digitaal forensisch archief (digitale inbeslagnames) zag het COC een probleem in de manier van werken van de politiezone omdat deze, naar het oordeel van het COC, niet beantwoordt aan de vigerende wetgeving, de richtlijnen van de Directie van de politionele informatie en de ICT-middelen (DRI) en het beheer van gegevens volgens de internationaal geldende veiligheidsnormen.

Daarnaast en subsidiair stelde het COC vast dat antwoordtermijnen overschreden werden en relevante gegevens in die antwoorden door de politiezone weggelaten werden.

Daarop en om die reden besloot het COC een beperkt toezicht te doen.

4. Het opzet van het beperkte toezicht bestaat erin:

- na te gaan of aan de wettelijke bepalingen van de titel 2 van de Wet op de Gegevensbescherming van 30 juli 2018 (WVG) en de Wet op het Politieambt van 5 augustus 1992 (WPA) is voldaan, evenals de regels op de informatieveiligheid zoals, niet limitatief, de dwingende Ministeriële richtlijn van 13 juli 2021[11], de brief van 01 februari 2023 van de Minister van Binnenlandse Zaken betreffende de "*Informatieveiligheid, veiligheid van de informatiesystemen en verwerkingsmodaliteiten van de politionele informatie*" en de richtlijnen voor de Geïntegreerde politie (GPI) zoals deze op hun communicatieplatform (Interne Sharepoint Bpol) gecommuniceerd worden;
- de communicatie door de politiezone tegen het licht te houden uit hoofde van de wettelijke termijn van de melding van de *data breach* en het tijdsverloop enerzijds en de aangeleverde documenten anderzijds;
- het schetsen van het wettelijk kader rond het beheer en de beveiliging van de informatie. Hierbij worden zowel de richtlijnen als de bronnen naar deze richtlijnen weergegeven;
- de chronologie van de aanmelding en relevante vragen en antwoorden uit het oorspronkelijk dossier DB230034 te evalueren.

Op 5 april 2024 werd het ontwerprapport voor prelectuur en, in voorkomend geval, opmerkingen naar de PZ WVL overgemaakt met het oog op het organiseren van tegenspraak.

Bij e-mail van 7 mei 2024 van de korpschef van de PZ WVL werden de opmerkingen en/of suggesties op het ontwerprapport ontvangen en, waar opportuun, verwerkt in huidig eindrapport.

5. ONDERZOEKSBEVINDINGEN

5. Op 12 november 2023 deed de PZ WVL een aanmelding van een *data breach* bij het COC m.b.t. het verlies van data van digitale inbeslagnames van het volledige jaar 2022 door een menselijke fout[12]. De relevante elementen uit de aanmelding zijn de volgende (stuk 1)

- Op 31 oktober 2023 rond 11:00 uur deed zich een incident voor omschreven als : *"LIK medewerker wenste een aanpassing te maken aan een dossier, en verwijderde[13] de folder "digitale inbeslagnames van 2022"."*
- Als "*Verdere stappen*" vermeldt het aanmeldformulier *: "De medewerker heeft de dienst ICT en zijn diensthoofd onmiddellijk op de hoogte gebracht, waarbij de ICT dienst in eerste instantie geprobeerd heeft om de data te recupereren. Zij hebben volgende acties ondernomen:*
    - *Lokale prullenbak nagekeken, zonder resultaat*
    - *Ctrl-Z geprobeerd, zonder resultaat*
    - *SMB-share en xxx storage bevatten geen prullenbak*

[11] Gemeenschappelijke dwingende richtlijn van de Ministers van Justitie en van Binnenlandse Zaken met betrekking tot de maatregelen die nodig zijn om het beheer en de veiligheid, waaronder in het bijzonder de aspecten met betrekking tot de betrouwbaarheid, de vertrouwelijkheid, de beschikbaarheid, de traceerbaarheid en de integriteit van de persoonsgegevens en de informatie die worden verwerkt in de gegevensbanken bedoeld in artikel 44/2 van de Wet op het Politieambt, te verzekeren, *B.S.*, 13 juli 2021.
[12] COC Dossier DB230034.
[13] Onderlijnd door het COC.

- *Contact opgenomen met xxx, de leverancier van het systeem, om na te gaan hoe de informatie gerecupereerd kon worden doch dit blijkt niet mogelijk te zijn"*

- Volgens het aanmeldingsformulier werd dit incident 10 dagen later op 9 november 2023 gedetecteerd op het tweewekelijks ICT overleg, waarna er melding gedaan werd aan het COC.
- De impact werd door de PZ WVL omschreven als volgt :
  - "*Digitaal in beslaggenomen materiaal, dat dienst doet als bewijs in een strafrechtelijk dossier, voor de dossiers aanhangig gemaakt in 2022 zijn niet langer beschikbaar op de xxx server.*
  - *De digitale inbeslagname bevat uitlezingen van digitale dragers, bankonderzoeken en beeldmateriaal.*
  - *In totaal gaat het om 502 processen verbaal, een combinatie van aanvankelijke en navolgende PV's. Het aantal unieke dossiers zijn nog niet gemapped."*
- Deze impact moet in combinatie gezien worden met het aantal betrokkenen zoals door de PZ WVL gedetecteerd : "*Iedere persoon betrokken in een strafrechtelijk vooronderzoek waarvan het dossier werd neergelegd bij de griffie in het jaar 2022 en waarvan het dossier digitaal bewijsmateriaal bevat."* Echter, de betrokkenen worden op het moment van de melding niet geïnformeerd omdat ze "*Niet gedefinieerd op dit ogenblik*" zijn.
- Deze melding werd door de PZ WVL zelf geclassificeerd als een "*Melding in verschillende stappen - Eerste melding*", waarbij het COC er bijgevolg van uit ging dat de PZ WVL de intentie had om zelf nog nadien bijkomende gegevens te verstrekken als deze bekend zouden worden.

6. Het COC stelde daarop bijkomende vragen. De verdere communicatie per mail van 30 januari 2024 (stuk 4) tussen de PZ WVL en het COC toont aan dat er geen *back-up* genomen werd van de verloren informatie. Uit deze mail blijken volgende relevante opmerkingen en vaststellingen :

- Aangaande de verantwoordelijkheid voor het niet voorzien van een *back-up*. De letterlijke vraag van het COC : "*U stelt dat de back-up niet geïmplementeerd werd omwille van het kostenplaatje. Kan u de documenten die deze beslissing staven aan ons overmaken : wie heeft de beslissing genomen en wie neemt hiervoor de verantwoordelijkheid.".* Het antwoord van de PZ WVL luidt, *verbatim*, als volgt "*De korpschef neemt hiervoor de verantwoordelijkheid. De beslissing werd niet gedocumenteerd. Tijdens de wekelijkse bespreking tussen ICT en de Directie Beheer worden de prioriteiten mondeling besproken. Afhankelijk van de noden binnen de verschillende diensten op vlak van ICT en de vooropgestelde budgetten van de politiezone wordt een afweging gemaakt of deze al dan niet voorgelegd wordt in het directiecomité. In essentie wordt er jaarlijks een budget voorzien voor de vernieuwing van de ICT-infrastructuur, zowel wat betreft connectiviteit als serverinfrastructuur; vernieuwing van hardware zodat onze medewerkers optimaal kunnen werken (pc's, schermen, ...); en de investering in software licenties die helpen onze mensen efficiënter hun taak uit te oefenen (vb. software tools aangewend voor forensisch onderzoek LCCU); ...* "
- Op de vraag in voormelde mail van 30 januari 2024 naar de back-up met de letterlijke vraag van het COC : "*In uw schema's staat een xxx back-up server. Mogen we begrijpen dat deze niet werd aangekocht of wordt deze voor andere back-ups gebruikt ?*", antwoordt de politiezone: "*De xxx back-up werd aangekocht, en dient als back-up voor enerzijds de architectuur van de digitale servers, en anderzijds de data van de fileserver(s). Een gedetailleerd overzicht kunt u terugvinden via de OneDrive link. Er wordt geen backup gemaakt van de data die geregistreerd staat op de server, dit omvat de beelden van de ANPR-camera's, bodycams en het digitaal forensisch archief."*

7. Het COC stelde ook vast dat de communicatie met de PZ WVL moeizaam verliep wat zich heeft geuit in de volgende vaststellingen:

- documenten werden aangeleverd waaruit evenwel bleek dat informatie ontbrak die relevant is voor het zorgvuldig uitvoeren van het onderzoek van de *data breach*;
- de termijnen die verlopen tussen de vaststelling van de *data breach* door de PZ WVL en de melding ervan;
- de vraag over welke gegevens het precies gaat – geen identificatie van betrokkenen;
- de redenen en motivering die werd opgeven voor het niet voorhanden hebben van een *back-up* systeem.

6. JURIDISCH KADER

6.1. Inleiding

8. Voor het beheer en de beveiliging van informatie bestaat er een regelgevend kader. In wat volgt wordt dit regelgevend kader beknopt weergegeven met de focus op de verplichting om *back-ups* te hebben:

- de WVG van 30 juli 2018, inzonderheid de artikelen 50-51 en 60 (de verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen);
- *LED* 2016/680, inzonderheid de overweging 53;
- de Ministeriële dwingende richtlijn[14] van 13 juli 2021;
- deze Ministeriële richtlijn is gebaseerd op het document "*Baseline Information Security Guidelines*" (BSG) van het *Center for Cyber Security Belgium* (*CCB*) dat tevens ingaat op *back-up*;
- de brief van 1 februari 2023 van de Minister van Binnenlandse Zaken betreffende de "*Informatieveiligheid, veiligheid van de informatiesystemen en verwerkingsmodaliteiten van de politionele informatie*"[15] gericht aan de commissaris-generaal en alle korpschefs van de lokale politie,
- richtlijnen rond informatiebeheer GPI[16] met specifieke aandacht voor *back-up*;
- internationale standaarden gebruikt in bovenstaande documenten ISO 27k.

6.2. Inbreuk op de beveiliging of *data breach*

9. Artikel 26, 11° van de WVG omschrijft een "*inbreuk op de beveiliging"* (*data breach*), als "*een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde bekendmaking of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens*".

10. De WVG gaat in parlementaire werken betreffende de artikelen 60-62 verder in op gegevensverlies (*data breach*) en stelt hierover het volgende: *"Een inbreuk op de beveiliging kan, wanneer deze niet tijdig en adequaat wordt aangepakt, resulteren in lichamelijke, materiële of immateriële schade voor natuurlijke personen, zoals verlies van controle over hun persoonsgegevens of beperking van hun rechten, discriminatie, identiteitsdiefstal of -fraude, financiële verliezen, ongeoorloofde ongedaanmaking van pseudonimisering, reputatieschade, verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens, of enig ander aanzienlijk economisch of maatschappelijk nadeel voor de natuurlijke persoon in kwestie."*

6.3. Passende technische en organisatorisch maatregelen

11. Op grond van artikel 50 WVG moet de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen nemen om de risico's voor de bescherming van de rechten en de vrijheden van de betrokkenen te waarborgen. Hoewel daarbij rekening wordt gehouden met de stand van de techniek en de uitvoeringskosten (parlementaire werken bij artikel 51 § 1 WVG), "(mag) *De tenuitvoerlegging van die maatregelen niet alleen van economische overwegingen afhangen*".

Daarnaast stelt artikel 60 § 2, 2° WVG dat de verwerkingsverantwoordelijke de nodige "*maatregelen* (neemt) *om te verhinderen dat onbevoegden de gegevensdragers kunnen, lezen, kopiëren, wijzigen of verwijderen*[17]".

---

[14] Gemeenschappelijke dwingende richtlijn van de Ministers van Justitie en van Binnenlandse Zaken met betrekking tot de maatregelen die nodig zijn om het beheer en de veiligheid, waaronder in het bijzonder de aspecten met betrekking tot de betrouwbaarheid, de vertrouwelijkheid, de beschikbaarheid, de traceerbaarheid en de integriteit van de persoonsgegevens en de informatie die worden verwerkt in de gegevensbanken bedoeld in artikel 44/2 van de Wet op het Politieambt, te verzekeren.

[15] Op pagina 4 van deze brief, en met name onder "*Algemeen Kader*", 4e en laatste kolom, onder "*Technologische middelen*" wordt als 7e van de 9 technische middelen "*back-ups*" expliciet vermeld.

[16] Onder andere https://bpolb.sharepoint.com/sites/WiKiPolDataprotection-PSI_nl/SitePages/TECH_OPS_BACKUP.aspx

[17] Onderlijnd door het COC.

12. In dit verband moet tevens de aandacht worden gevestigd op artikel 60 § 2, 9° WVP. Deze bepaling legt aan de verwerkingsverantwoordelijke de plicht op om "*ervoor te zorgen dat de geïnstalleerde systemen in geval van storing opnieuw kunnen worden ingezet*". Deze zorgplicht brengt onder andere met zich dat er wordt voorzien in een *back-up* systeem zodat, bij onbeschikbaarheid of verlies van de gegevens op de gegevensdrager, de gegevens alsnog toegankelijk zijn op een andere gegevensdrager.

De Memorie van toelichting bij artikel 60 van de WVG (DOC 54/3126[18]) gaat op p. 105 verder in op deze verplichting en verwijst naar ISO 27000, waardoor de inhoud van deze normen ook van toepassing moet.

6.4. De relevante ISO-normen

13. De basisnormen waarop de regelgeving zich baseert, zijn de ISO-normen vanaf 27000. Het gaat hier over een verzameling van normen die allen beginnen met het nummer 'ISO 27000' en daarom worden aangeduid als 'ISO 27k'. De richtlijnen en aanbevelingen (*cf. supra*) verwijzen naar deze normen. Er wordt echter niet verwacht dat elke professional zelf deze normen gaat analyseren en implementeren. Daarom worden ze vertaald in de bovenstaande richtlijnen. Ze dienen echter wel als een basis en zijn internationaal erkend.

Hoewel dit industrienormen zijn, worden deze expliciet door de wetgever aangehaald, zoals in de Memorie van toelichting bij de Wet Gegevensbescherming (DOC 54/3126, pagina 105 aangaande art. 60 WVG).

Ook de WikiPol Dataprotection pagina op de interne website (Sharepoint GPI) van de politie verwijst naar deze normen.

6.5. De wet op het politieambt (WPA)

14. De verplichting met betrekking tot betrouwbaarheid, vertrouwelijkheid, beschikbaarheid, traceerbaarheid en de integriteit van persoonsgegevens wordt ook geregeld door art 44/4 §2 van de WPA die deze invulling onmiddellijk delegeert naar een dwingende ministeriële richtlijn. De vigerende dwingende ministeriële richtlijn waarvan sprake, materialiseert zich in de hogervermelde dwingende richtlijn van 13 juli 2021.

6.6. Ministeriële dwingende richtlijn[19] van 13 juli 2021

15. Deze Ministeriële richtlijn is "dwingend", wat betekent dat deze richtlijn niet als louter indicatief kan worden beschouwd, maar een juridische verplichting inhoudt in hoofde van de geadresseerde. De richtlijn richt zich in zijn aanhef o.a. tot de korpschefs. "*De korpschefs voor de lokale politie en de commissaris-generaal, de directeurs-generaal en de directeurs voor de federale politie staan borg voor de goede uitvoering van deze richtlijnen voor wat de gegevensbanken bedoeld in artikel 44/2, §§ 1 en 3 WPA, betreft.*". In deze kan dus gesteld worden dat de korpschef de (ook juridische) verantwoordelijkheid draagt in het uitvoeren – of minstens toezicht uitoefenen op de uitvoering en toepassing – van deze richtlijn. De korpschef draagt hierin de eindverantwoordelijkheid.

16. Het toepassingsgebied omvat tevens de politionele gegevensbanken waarin digitale inbeslagnames bewaard worden.

17. Deze richtlijn stelt expliciet "*De politiediensten voorzien de nodige bescherming van de informatie en de gegevens die zij verwerken tegen verlies, ongeoorloofde wijziging of vernietiging, hetzij per ongeluk hetzij door een moedwillige handeling.*".

18. Deze "*bescherming*" wordt ook in de richtlijn expliciet gemaakt onder punt "*9) De operationele veiligheid*". We citeren:

---

[18] www.dekamer.be, https://www.dekamer.be/FLWB/PDF/54/3126/54K3126001.pdf

[19] Gemeenschappelijke dwingende richtlijn van de Ministers van Justitie en van Binnenlandse Zaken met betrekking tot de maatregelen die nodig zijn om het beheer en de veiligheid, waaronder in het bijzonder de aspecten met betrekking tot de betrouwbaarheid, de vertrouwelijkheid, de beschikbaarheid, de traceerbaarheid en de integriteit van de persoonsgegevens en de informatie die worden verwerkt in de gegevensbanken bedoeld in artikel 44/2 van de Wet op het Politieambt, te verzekeren.

"*De minimale technische maatregelen die voor de ICT-middelen van de politiediensten genomen moeten worden(6), zijn:*
…
- back-up en business continuity (Operationele veiligheid) procedures."

6.7. WikiPol Dataprotection

19. Ook de DRI geeft enkele richtlijnen hoe de GPI moet omgaan met data. Relevant voor dit rapport is de aanbeveling 'D.1.12 Back-up van informatie'[20]. Deze aanbeveling stelt *expressis verbis*: "*Er worden onder meer uitvoerige back-ups gemaakt, de back-upmedia zijn adequaat en de integriteit van de back-ups wordt met regelmatige tussenpozen gecontroleerd om ervoor te zorgen dat alle informatie en alle software kunnen worden hersteld in geval van een incident, een mankement of het verlies van de back-upmedia.*"

Deze WikiPol Dataprotection aanbeveling steunt sterk op de ISO 27k-normen (*cf. supra*).

6.8. Center for Cyber Security Belgium : Baseline Information Security Guidelines (*BSG*)

20. De dwingende ministeriële richtlijn vermeldt expliciet de *BSG* als startpunt van de richtlijn. Het is dus zinvol om naar de bron te kijken en meer bepaald wat de *BSG* rond het omgaan met *back-up* van gegevens vermeldt.

Deze zijn in de richtlijn terug te vinden in de "*De minimale technische maatregelen die voor de architectuur worden genomen,* (zijn)", waarin, bij de minimale toe te passen maatregelen, het "*Beschikken over back-upprocedures: maken, testen van restauratie.*", wordt voorzien.

Niettegenstaande dit absoluut minimale maatregelen zijn, merkt het Controleorgaan op dat deze alvast veel verder gaan dan het louter 'hebben' van een *back-up*. Ook het (regelmatig) testen van de restauratie is hierin begrepen.

7. BEOORDELING

7.1. Chronologisch verloop van de relevante feiten na de melding van de *data breach* met COC referte DB230034

21. Het COC verleende ontvangstmelding bij mail op 13 november 2023 (stuk 2). Hierin werden bijkomende vragen gesteld met antwoordtermijn op 3 december 2023.
Hierop volgden vragen naar verduidelijking door het COC op 5 december 2023 (stuk 3). Deze verduidelijkingen hadden vooral te maken met:

- het feit dat gegevens uit de doorgestuurde documentatie 'verborgen'[21] werden;
- dat er gesteld wordt dat er bewust géén *back-up* genomen wordt van het digitale archief. Het gaat ter zake om "*uitlezingen van digitale dragers, bankonderzoeken en beeldmateriaal*"[22] verzameld en bewaard in het kader van vooronderzoeken (stuk 1).

Gezien de eindejaar periode werd de antwoordtermijn op 5 weken geplaatst.

22. Op 10 januari 2024 stuurde het COC een herinneringsmail met een nieuwe datum op 23 januari 2024. Op 22 januari 2023 ontving het COC bericht dat er nog geen overleg met de korpschef had plaatsgevonden. Uiteindelijk bereikten de antwoorden op de vragen van 5 december 2023 het COC op 30 januari 2024 (stuk 4).

In wat volgt plaatsen we de informatie van de PZ WVL naar aanleiding van het dossier DB230034 in evidentie met de hoger aangegeven regelgeving en aanbevelingen. Verder kijken we naar de antwoordtijden en het ontbreken van voor het COC relevante gegevens om de *data breach* te kunnen onderzoeken.

---

[20] https://bpolb.sharepoint.com/sites/WiKiPolDataprotection-PSI_nl/SitePages/TECH_OPS_BACKUP.aspx

[21] Deze gegevens zijn interne IP adressen en namen van externe projectmedewerkers in het document dat de architectuur en het project beschrijft. Het COC heeft vanuit zijn bevoegdheden nochtans de volledige toegang tot **alle** gegevens (artikel 244 §1 WVG).

[22] Blijkens de aangifte van de *data breach.*

1. RAPPORT

23. Tijdens het toezichtonderzoek werd door de PZ WVL opgemerkt dat een *back-up* van het digitale archief en het beeldmateriaal een extra kost van 180 KEUR (stuk 1, stuk 2, stuk 3) en/of 200 KEUR (stuk 5) zou betekenen. Dit werd tijdens het onderzoek door de PZ WVL initieel aangegeven als een reden waarom niet werd en zou worden voorzien in een back up van het digitaal archief.

De PZ WVL haalt daarbij de volgende elementen aan (letterlijke weergave, stuk 5):

> *Er werd geoordeeld dat de impact van het risico op dataverlies, minimaal was conform artikel 29, richtlijn EU 2016/680 (waarschijnlijkheid en ernst uiteenlopende risico's) omgezet in artikel 51 WVG, omwille van de beperkte toegang tot deze xxx server, en de werknemers die rechten hebben om hierop te schrijven.*
>
> *Het niet hebben van een back-up in deze specifieke context, werd bepaald deels door economische overwegingen, maar evenzeer door het type data die hier bewaard wordt.*
>
> *Er werd een afweging gemaakt voor het type data waarvoor een back-up noodzakelijk is.*
>
> *De verloren data van het digitaal archief bestaat uit de reeds neergelegde stukken bij de griffie. De omschrijving van deze data bestaan uit printscreens, uitgeschreven data van de uitlezingen en fotomateriaal die toegevoegd zijn in de processen-verbaal. De processen-verbaal worden beheerd, bewaard en geback-upt in het systeem van de lokale politie. Bijkomend wordt een volledig exemplaar bijgehouden in een digitaal archief xxx.*

Het COC kan deze redenering niet bijtreden omwille van de verschillende elementen en argumenten die in dit rapport uiteengezet worden, waaronder :

- de economische overweging kan op zich niet worden ingeroepen als een afdoende reden om geen *back-up* te voorzien;
- de impact van het dataverlies naar het oordeel van het COC, om de in dit rapport aangehaalde redenen, wel degelijk ernstig is;
- er ligt geen bewijs voor dat het verloren digitaal archief **uitsluitend** bestaat uit reeds ter griffie neergelegde stukken en processen-verbaal. Op dat vlak lijkt er trouwens een tegenstrijdigheid te zijn[23]in de repliek van 6 mei 2024 van de PZ WVL (stuk 5);
- de uiteindelijke opname van de processen-verbaal, na verloop van een zekere tijd (de tijd nodig op de processen-verbaal op te stellen en af te werken, vervolgens over te maken aan het parket en nadien te archiveren in xxx), niet als volwaardig alternatief van een rechtstreekse *back-up* van het digitale archief kan beschouwd worden;
- het verlies van de data hoe dan ook een procedurele of strafvorderlijke impact heeft of kan hebben in die zin dat bij bijvoorbeeld betwistingen over de (correcte) inhoud van een proces-verbaal geen (bijkomend) onderzoek meer kan bevolen worden (zowel tijdens het vooronderzoek als tijdens het onderzoek ter terechtzitting), vermits de originele data, die de bron waren voor het opstellen van de processen-verbaal verloren zijn gegaan[24]. Die (negatieve) impact kan zowel ten nadele van het Openbaar Ministerie, van de verdachte (n) of van de burgerlijke partij(en) of slachtoffer(s) zijn (zie ook verder onder randnummer 34);
- de beperkte toegangsrechten maar pas nuttig zijn indien er een *principle of least privilege* geïmplementeerd wordt. Bij het *principle of least* privilege zijn er vooraf duidelijk bepaalde rollen waarvan de gebruiker (*user*) één rol uit de hem toegekende rollen aanneemt met slechts de rechten die absoluut noodzakelijk zijn voor de taken die hij op dat ogenblik dient uit te voeren. Dit impliceert enerzijds dat deze rollen duidelijk bepaald en gescheiden zijn en anderzijds dat personen tijdelijk van rol dienen te wijzigen voor toegangen die een hoger of ander prioriteitsniveau vereisen zoals het wissen van gegevens.

[23] Langs de ene kant wordt immers op blz. 2 gesteld (voorlaatste §): "*De verloren data van het digitaal archief bestaat uit de reeds neergelegde stukken bij de griffie*", terwijl op blz. 3 wordt gesteld (3e §, 3e streepje: "*Digitaal archief: omvat alle bewijsvoering die **niet** kan neergelegd worden bij de griffie, en die opgeroepen kan worden tijdens de zitting*".)

[24] Dat wordt ook impliciet bevestigd door de PZ WVL in de repliek van 6 mei 2024 (stuk 5) waar op blz. 3 wordt gesteld (3e §, 3e streepje): "*Digitaal archief: omvat alle bewijsvoering die niet kan neergelegd worden bij de griffie, **en die opgeroepen kan worden tijdens de zitting**".* Het is niet alleen "tijdens de zitting", maar ook tijdens het hele vooronderzoek dat die mogelijkheid zich kan voordoen.

Hoewel het COC begrijpt dat het installeren van een *back-up* (aanzienlijke) kosten met zich mee kan brengen, kan er niet worden voorbijgegaan aan de verantwoordelijkheid die ter zake op de verwerkingsverantwoordelijke, *in casu* de PZ WVL, rust, om in een *back-up* te voorzien zoals door de regelgeving wordt voorgeschreven.

In de finale fase van de tegenspraak wordt uiteindelijk door de PZ WVL het volgende gesteld (letterlijk): "*We hebben de laatste jaren al veel moeten rationaliseren op de uitgaven maar we zijn zeker bereid om de aankoop van de extra backup-server (geschat rond de 200.000 €) voor de toekomst in overweging te nemen (eigen onderlijning). Een en ander zal moeten overlegd worden met de bestuurlijke overheid*" (stuk 5). Hieruit kan alleszins afgeleid worden dat de kwestie nooit eerder en nog niet is of werd voorgelegd aan de bestuurlijke overheid.

7.2. Tijden voor melding en antwoorden

24. Volgens de aanmelding deed het incident zich voor op 31 oktober 2023, rond 11:00 uur. Hoewel de aanmelding vermeldt dat dit incident 'onmiddellijk' werd gemeld (stuk 1), duurde het toch tot 9 november 2023 alvorens deze *data breach* op het intern overleg "*tweewekelijks overleg met de ICT dienst met betrekking tot lopende zaken, en over de vastgestelde incidenten en hoe deze verholpen werden*" bij de PZ WVL werd besproken en vervolgens nog eens tot 12 november 2023 alvorens melding gedaan werd aan het COC. Nochtans dienen *data breaches* binnen de 72 uur na de vaststelling gemeld te worden[25]. **De PZ WVL gaf in zijn aanmelding geen verdere toelichting waarom dit incident pas na 2 (twee) weken in plaats van 72 uur werd aangemeld**.

25. Op 5 december 2023 stuurde het COC een vraag naar verdere inlichtingen. Het COC tracht hier steeds een redelijke termijn te hanteren en voorzag de opvolging op 5 (vijf) weken omwille van de eindejaar periode. Dat wil zeggen dat er uiterlijk op 10 januari 2024 een antwoord verwacht werd. Wanneer dit antwoord er niet kwam, stuurde het COC een herinneringsmail en legde een supplementaire antwoordtijd van 2 (twee) weken vast, met uiterste datum 23 januari 2024. Op 22 januari 2024 reageerde de PZ WVL dat deze datum niet haalbaar was en uiteindelijk kwam er antwoord op 30 januari 2024.

Het COC stelt vast dat de PZ WVL het Controleorgaan bijna 2 (twee) maanden op een antwoord liet wachten.

7.3. Het ontbreken van gegevens

26. In de communicatie van de PZ WVL werd aan het COC het document toegestuurd met de architectuur en het project rond de invoering van de xxx infrastructuur. Bij het openen van de documenten merkte het COC echter dat er gegevens uit dit document verborgen werden gehouden, zonder dat daarvoor minstens een verantwoording werd verleend.

In concreto gaat het over IP adressen en de namen van de (externe) projectmedewerkers (verwerkers van de politiezone derhalve). Deze gegevens kunnen in een latere fase nochtans hun belang hebben bij de verdere verificaties zoals afscherming en segregatie van het netwerk en betrokken externe partijen en de adviezen die deze gegeven zouden kunnen hebben bij het opstellen van de architectuur en de aangekochte apparatuur.

27. Behoudens de uitzonderingen voorzien in artikel 245 § 2, 2de lid, laatste zinsdeel (informatie m.b.t. een lopend opsporings- of gerechtelijk onderzoek of de bescherming van de fysieke integriteit) WVG, heeft het COC toegang tot **alle informatie** waar het om verzoekt krachtens artikel 244 §1 WVG. Evenwel werden geen van deze uitzonderingen door de PZ WVL ingeroepen en lijken zij ook niet te kunnen worden ingeroepen.

28. Na expliciete vraag van het COC werden de documenten met alle gegevens overgemaakt.

Aanbeveling 1

Het transparant documenteren en communiceren naar belanghebbenden van beslissingen met gevolgen voor de databescherming in het algemeen en ICT-gerelateerde werkwijzen in het bijzonder.

In het kader van de tegenspraak stelt de PZ WVL het volgende (stuk 5, letterlijke weergave) :

[25] *LED* overweging 61 en artikel 30/1 omgezet in artikel 61 §1 WVG.

- *"We zijn akkoord dat we hier verdere inspanningen dienen te leveren met betrekking tot een meer risico geanalyseerde aanpak, waarbij het duidelijk dient te zijn wat we beschouwen als kritisch en wat niet. Vorig jaar werd in het budget opgenomen om een audit uit te voeren en een pentesting om de zwakheden in kaart te brengen van onze ICT-systemen (deze beslissing werd nog ruim voor het incident genomen, net omdat we een goed zicht willen krijgen op de kritische elementen binnen onze informatiehuishouding)".*
- *"Naar aanleiding van de output van deze audit, hebben we besloten om het veiligheidsplan uit te werken en hierbij de dringende acties af te werken. Dit, rekening houdend met de wetgeving waarin ook u verwijst in dit rapport en met als hulpkit de cyfun tools aangereikt door het CCB. Hierbij wordt ondersteuning geboden van een extern consulent".*

Het COC neemt akte van de door de politiezone meegedeelde in uitvoering zijnde en voorgenomen maatregelen.

7.4. Definitie van het begrip "*back-up*"

29. Het begrip *back-up* is een technisch begrip dat er in bestaat om opgeslagen gegevens in de toestand waarop ze zich op een bepaald moment bevinden op een andere gegevensdrager te bewaren zodat bij een calamiteit zoals verlies, beveiligingsincident (virus, onbeschikbaarheid door hardware falen, ransomware, menselijke fout waardoor de gegevens gewijzigd of verwijderd worden, enz. …) de gegevens kunnen 'terug gehaald' worden naar de toestand waarop het zich op het moment van de *back-up* bevond. Een *Back-up* beperkt zich bovendien niet tot een vorige versie maar gaat ook meerdere versies terug in de tijd.

30. Het begrip *back-up* mag niet verward worden met *high-availability* en '*redundantie'*, waar men zorgt dat systemen beschikbaar blijven, ook als een deel van de hardware faalt. Immers, gegevens die uit een systeem met maatregelen om hoge beschikbaarheid te garanderen gewist of gewijzigd worden, verdwijnen uit het systeem en kunnen dan enkel nog met een *back-up* terug hersteld worden.

31. In deze zin ziet het COC de '*xxx server*' van PZ WVL als een systeem met hoge beschikbaarheid, maar zonder de noodzakelijke maatregelen voor *back-up* voor de hier aangehaalde gegevens betreffende het digitale archief en het beeldmateriaal.

32. De toepasselijke wet- en regelgeving verwijzen in deze context naar "*technische en organisatorische maatregelen*" om beschikbaarheid te garanderen en verlies tegen te gaan.

7.5. Back-up

33. Zoals de juridische bronnen (dwingende ministeriële richtlijn van 13 juli 2021), de interne richtlijnen voor de politie (WikiPol), de overheidsaanbevelingen (BSG van het Center voor Cybersecurity Belgium) en de internationale standaarden (ISO 27k) voorschrijven is het nemen van een *back-up* niet enkel een gebruikelijke voorzorg voor het beheren van informatie, maar zondermeer een wettelijke verplichting. De PZ WVL geeft in zijn antwoorden expliciet aan ervoor te kiezen om **niet** aan deze verplichtingen te voldoen voor wat betreft : "*beelden van de ANPR-camera's, bodycams en het digitaal forensisch archief."* (stuk 3).

34. Ten aanzien de strafrechtelijke opsporing en vervolging kan het verlies van digitale inbeslagnames (zware) gevolgen hebben voor het strafonderzoek (opsporingsonderzoek/gerechtelijk onderzoek en desgevallend onderzoek ter terechtzitting), enerzijds, en de rechten van de verdediging anderzijds omdat de aantoonbaarheid van de feiten door het verlies van de (potentiële) bewijs- en overtuigingsstukken, niet meer mogelijk is. Ook eventuele slachtoffers kunnen daar potentieel de nefaste gevolgen van dragen voor zover de opsporing en vervolging door het verlies van de data onmogelijk dan wel sterk bemoeilijkt is geworden. Het COC kan alleen maar hopen dat de strafvorderlijke (en burgerrechtelijke) gevolgen binnen aanvaardbare perken is gebleven maar heeft daar verder geen concreet zicht op.

In het raam van de tegenspraak benadrukt de PZ WVL dat er voor andere systemen wel *back-ups* worden genomen. Hoewel het COC akte neemt van de opmerking van de PZ WVL, moet evenwel worden opgemerkt dat enkel het dataverlies van het digitaal forensisch archief het voorwerp van het toezichtonderzoek uitmaakt zodat andere verwerkingssystemen van de PZ WVL hier buiten beschouwing worden gelaten.

Aanbeveling 2

Het voorzien van maatregelen door de PZ WVL om de informatieveiligheid te garanderen en *in casu* dataverlies tegen te gaan zoals *back-ups* in overeenstemming met alle (hoger vermelde) vigerende regelgeving en industrienormen.

In het kader van de tegenspraak stelt de PZ WVL het volgende (stuk 5, letterlijke weergave):

> • *"Zoals in de communicatie met betrekking tot het verlies van de data, kan geen enkel operationeel lid nog wegschrijven op de xxx server. De bestanden geschreven naar het digitaal archief, worden door het LIK geplaatst in een folder op hun NAS, en deze worden weggeschreven via een script naar de xxx. Na 24u is het enkel nog mogelijk om deze bestanden te lezen".*
>
> • *"…".*

Met deze opmerking geeft de PZ WVL aan dat de verloren data van de digitale inbeslagnames 'niet kritisch' zouden zijn. Immers, anders zouden ze wel opgenomen zijn in het *back-up* schema. Het COC volgt de redenering van de PZ WVL niet dat deze data 'niet kritisch' zouden zijn. Bij de digitale inbeslagname worden diverse gegevens verzameld en deze worden al dan niet verwerkt in de gerechtelijke dossiers. Bij deze verwerking worden er (vaak slechts) selecties gemaakt, wat impliceert dat niet (of zelden) **alle** gegevens worden overgemaakt en vaak worden gegevens "verwerkt" (samengevat, enkel de meta-data, enz. …). Zoals hoger vermeld, kan het nodig zijn om tijdens de het vooronderzoek of het onderzoek ter terechtzitting (eerste aanleg, beroep, beroep na cassatie) terug te grijpen naar de oorspronkelijke gegevens omwille van de bewijskracht, bewijsdiscussies, verdere contextualisatie, dieper onderzoek, verduidelijking, enz. … Het COC blijft dus bij zijn oordeel dat deze data wel degelijk 'kritische data' is en derhalve dient opgenomen te worden in de *back-up*.

7.6. Antwoordtijden

35. Na de aanmelding van het incident stelde het COC vast dat de PZ WVL zeer lang wachtte om te antwoorden op de vragen van het COC. De omvang van het incident, *in casu* wat bij de aanmelding naar voren geschoven werd als mogelijk verloren bewijsmateriaal, deed echter uitschijnen dat de prioriteit die aan dit incident diende gegeven te worden van een hogere orde hoorde te zijn.

In het raam van de tegenspraak stelt de PZ WVL (stuk 5, letterlijke weergave):

> *"We dienen hier een kleine toevoeging te maken, de prioriteit bij de eerste melding was om u op de hoogte te brengen van het verlies van de gegevens. De late aanmelding gebeurde omdat initieel ervan uit was gegaan dat volledige recuperatie mogelijk was. Het verlies van de gegevens kwam tot stand door een menselijke fout waar geen malafide intentie aan verbonden was. Het is pas na overleg met verwerker en contact met xxx helpdesk dat duidelijk werd dat deze data niet gerecupereerd konden worden.*
>
> *De periode waarop diende geantwoord te worden op de bijkomende vragen viel ongelukkiger wijze in de feestperiode, waardoor het inderdaad moeilijk was om te aligneren met de verschillende betrokken personen. Het was een hele oefening om een correct aantal te krijgen van hoeveel dossiers er juist waren geïmpacteerd. Vandaag hebben we besloten om de zoektocht naar het bewijsmateriaal te stoppen, en het finale nummer door te geven aan het parket".*

Het COC vindt het belangrijk dat de wettelijke termijnen van de aanmelding (72 uur na het incident) gerespecteerd worden, ook al kan men later het gegevenslek "herstellen". Ook in de weerhouden antwoordtermijnen tracht het COC steeds realistisch te zijn; zo had het COC reeds rekening gehouden met de eindejaar periode (feestperiode) zoals uiteengezet in de randnummers 21 en 25. Met andere woorden, het COC merkt op dat het voor het aanmelden van de *data breach* op zichzelf niet relevant is of de gegevens kunnen gerecupereerd worden of niet; dit immers doet niets af aan het feit dat er sprake was van gegevensverlies.

Aanbeveling 3

Het implementeren van de processen die leiden tot het tijdig melden van een inbreuk op de gegevensbescherming zodanig dat er steeds een juiste en tijdige afhandeling gegarandeerd wordt.

In het kader van de tegenspraak stelt de PZ WVL (stuk 5, letterlijke weergave) :

- *"Vandaag is er een incidentrespons procedure en waarbij de procedure normaal is dat ….*
- *"Het verlies van de data heeft inderdaad de nood aangetoond dat het proces niet ingeburgerd is, en dat verdere bewustwording noodzakelijk is".*
- *"Dit wordt eveneens opgenomen in het veiligheidsplan, en zal tijd vragen om deel te worden van onze cultuur".*

Het COC neemt akte van de door de politiezone meegedeelde in uitvoering zijnde en voorgenomen maatregelen.

7.7. De bevoegdheid om gegevens te verwijderen

36. In randnummer 11, 2de alinea wordt verwezen naar artikel 60 § 2, 2° WVG, waaruit blijkt dat de PZ WVL de nodige maatregelen moet nemen om te verhinderen dat onbevoegden de gegevensdragers, onder meer, niet kunnen verwijderen. Deze plicht maakt deel uit van de algemene plicht om passende organisatorische en technische maatregelen te nemen om onder meer de integriteit en beschikbaarheid van de persoonsgegevens te beschermen. Beide waarborgen zijn gematerialiseerd in de Gemeenschappelijke bindende richtlijn van de Ministers van Justitie en van Binnenlandse Zaken "*met betrekking tot de toegangsregels van de leden van de politiediensten tot de algemene nationale gegevensbank en de basis-, bijzondere en technische gegevensbank*" van 10 juli 2021[26] en nader uitgewerkt in de niet openbaar bekend gemaakte fiche D41 van de MFO 3.

37. Hieruit volgt dat een lid van de GPI alleen wettig bevoegd is om toegang te hebben tot informatie en persoonsgegevens bedoeld in artikel 44/1 § 1 van de WPA, wanneer dit noodzakelijk en proportioneel is in functie van de rol die aan het lid wordt toegekend. De toegekende rol heeft ook een impact op de reikwijdte en de afbakening van de verwerkingsbevoegdheid waarvan welbepaalde verwerkingen wel of niet deel uitmaken. Het is evident dat de mogelijkheid om informatie en persoonsgegevens uit de politionele omgeving te **verwijderen** (wat voor alle duidelijkheid een verwerking is) niet aan ieder lid van de GPI (of *in casu* de politiezone) kan worden toegekend.

38. Een personeelslid kan op verschillende momenten verschillende rollen vervullen. Het kan daarom nodig zijn dat een personeelslid tussen deze rollen schakelt. Zo kan een personeelslid in de rol van 'LIK-medewerker' gegevens aanmaken en consulteren, maar niet verwijderen. Voor het verwijderen dient hij te schakelen naar de rol van '(systeem)beheerder/administrator' die hij niet permanent bekleedt, maar enkel gebruikt met een specifiek doel waarvoor deze rol noodzakelijk is. Ook de logging van de bewerkingen dient dan onder meer aan te tonen welke medewerker (wie) een bepaalde actie (wat) gedaan heeft op welk moment en in welke rol.

39. Het niet openbaar gepubliceerde ambtshalve advies DD210006 van het COC dd. 24 maart 2021 (beschikbaar op de interne Sharepoint GPI) betreffende het *"Advies uit eigen beweging betreffende het ontwikkelen van een profielenbeleid in het algemeen, het toekennen van het onderzoeksprofiel "gevorderde exploitatie" in het bijzonder aan de leden van de geïntegreerde politie en betreffende het gebruik van de toepassing ANG controle door de onthaalmedewerker."* stelt in deze:

*Het moet ook in herinnering gebracht worden dat de MFO 3 - een **dwingende** richtlijn voor **alle** politiediensten in de zin van art. 62, 6° Wet Geïntegreerde Politie van 7 december 1998 - in zijn fiche D41 onder meer het volgende stelt:*

> *- "Bij het toekennen van de toegangen tot de verschillende toepassingen zal rekening gehouden worden met de werkelijk uitgeoefende taken van het personeelslid en de operationele behoeften".*
>
> *- De verantwoordelijke zal bij het toekennen van de toegangen tot de verschillende toepassingen aan elk personeelslid een zo gepersonaliseerd mogelijke toegang tot de ANG verschaffen, in overeenstemming met de taken uitgeoefend door dit personeelslid".*

In deze geldt het toekennen van zo gepersonaliseerd mogelijke toegangen tot de ANG door middel van rollen *mutatis mutandis* voor alle andere politionele toepassingen en gegevensbanken.

Aanbeveling 4

Het duidelijk omschrijven van de toegang tot de systemen in rollen met voor elke rol enerzijds de noodzakelijke toegang, maar anderzijds zo weinig mogelijk toegang (*principle of least privilege*). Dit impliceert dat personen tijdelijk van rol

[26] *B.S.,* 13 juli 2021.

dienen te wijzigen voor toegangen die een hoger prioriteitsniveau vereisen zoals het wissen van gegevens. De vigerende (hoger vermelde) regelgeving en industrienormen zijn hierin leidend.

In het kader van de tegenspraak stelt de PZ WVL het volgende (stuk 5, letterlijke weergave):

- *"Er is een on en off boarding procedure waarbij de aanvragen voor toegang tot applicaties worden overlopen en besproken tijdens wekelijkse overleg alvorens deze toe te kennen en/of te wijzigen".*
- *"We voegen de procedures toe in de gedeelde OneDrive"*

Dit biedt echter geen antwoord op de aanbeveling om met rollen te werken en het *principle of least privilege* te implementeren.

8. BESLUIT

39. De regelgeving en richtlijnen zijn duidelijk: elk politioneel informaticasysteem dient te beschikken over afdoende informatieveiligheidsmaatregelen, zoals een *back-up*. Het *in casu* getroffen systeem van de PZ WVL valt hieronder en er had daarom een afdoende *back-up* moeten voorzien worden voor het digitaal forensisch archief.

40. De PZ WVL stelt dat de korpschef de keuze gemaakt heeft om geen *back-up* te installeren voor de *bodycams*, de ANPR camera's en het digitaal forensisch archief, en hij hiervoor de volledige verantwoordelijkheid neemt. Onafgezien van de draagwijdte van dit verantwoordelijkheidsbesef werd dit beslissingsproces evenwel niet gedocumenteerd en kan het kennelijk ook niet gestaafd worden. De argumentatie dat dit economisch niet haalbaar is, is niet enkel op grond van de vigerende wet- en regelgeving niet te weerhouden maar is, gelet op de potentieel zeer zware gevolgen, ook vanuit de figuur van de vroegere *bonus pater familias* (thans, de 'voorzichtig en redelijk persoon' in het Nieuw Burgerlijk Wetboek), niet te verdedigen.

41. Het verlies aan gegevens van het digitaal forensisch archief, met (potentieel) zware gevolgen voor de werking van Justitie en alle betrokkenen en belanghebbenden, had vermeden kunnen worden indien de politiezone de nodige inspanningen en stappen zou genomen hebben (ook ten aanzien van zijn politieoverheden) om een zo hoog mogelijk beschermingsniveau inzake informatieveiligheid van het digitaal forensisch archief te waarborgen. Het voorzien in een back-up van het digitaal forensisch archief is daarbij de evidentie.

42. Het COC merkt hierbij op dat bij de aanmelding van het incident de voorziene wettelijke termijnen niet werden gerespecteerd en er bovendien nadien onnodig veel tijd verstreken is voor het beantwoorden van de verschillende vragen naar informatie vanwege de toezichthouder.

43. Bovendien merkt het COC op dat in de eerste communicatie gegevens ontbraken niettegenstaande het COC volledige toegang moet krijgen tot **alle** beschikbare informatie.

44. Er moeten tot slot mechanismen worden opgezet waarbij een lid van de politiezone West-Vlaanderen niet zomaar informatie en persoonsgegevens uit een politionele gegevensbank kan verwijderen.

OM DEZE REDENEN,
Het Controleorgaan,

Doet de hiernavolgende aanbevelingen aan de politiezone West-Vlaanderen,

Aanbeveling 1

Het transparant documenteren en communiceren naar belanghebbenden van beslissingen met gevolgen voor de databescherming in het algemeen en ICT-gerelateerde werkwijzen in het bijzonder.

Aanbeveling 2

Het voorzien van maatregelen door de PZ WVL om de informatieveiligheid te garanderen en *in casu* dataverlies tegen te gaan zoals *back-ups* in overeenstemming met alle (hoger vermelde) vigerende regelgeving en industrienormen.

Aanbeveling 3

Het implementeren van de processen die leiden tot het tijdig melden van een inbreuk op de gegevensbescherming zodanig dat er steeds een juiste en tijdige afhandeling gegarandeerd wordt.

Aanbeveling 4

Het duidelijk omschrijven van de toegang tot de systemen in rollen met voor elke rol enerzijds de noodzakelijke toegang, maar anderzijds zo weinig mogelijk toegang (*principle of least privilege*). Dit impliceert dat personen tijdelijk van rol dienen te wijzigen voor toegangen die een hoger prioriteitsniveau vereisen zoals het wissen van gegevens. De vigerende (hoger vermelde) regelgeving en industrienormen zijn hierin leidend,

Beslist **geen actieve** opvolging te doen van bovenstaande aanbevelingen t.a.v. de politiezone West-Vlaanderen,

Brengt niettemin tegelijk ter kennis aan de (functioneel) verwerkingsverantwoordelijk politiezone West-Vlaanderen dat ze te allen tijde, conform de beginselen en verplichtingen van titel 2 van de Wet Gegevensbescherming, de naleving van de regels inzake gegevensbescherming en politioneel informatiebeheer moet kunnen aantonen aan het Controleorgaan, bijvoorbeeld n.a.v. een eventueel ander onderzoek of dossier of door het COC georganiseerde steekproeven.

Rapport door het Controleorgaan op de Politionele Informatie goedgekeurd op 11 juni 2024.

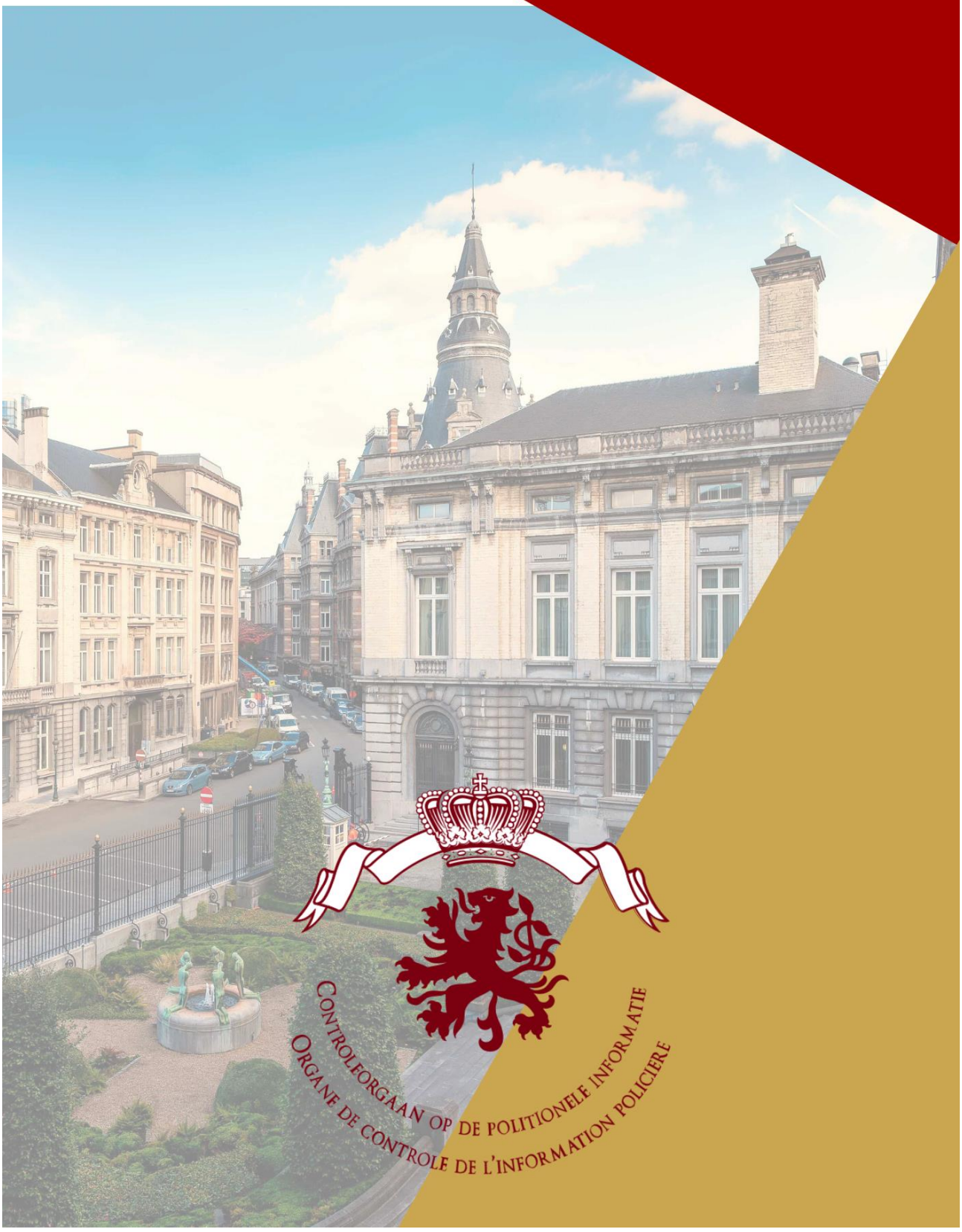
Afschrift aan:

- De burgemeester van en te West-Vlaanderen[27]
- De procureur des Konings van en te West-Vlaanderen[28]

Voor het Controleorgaan,

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

[27] Cf. Artikel 237, 3e lid Wet Gegevensbescherming.
[28] Cf. Artikel 237, 4e lid Wet Gegevensbescherming.



Controleorgaan op de politionele informatie

Organe de contrôle de l'information policière