VISITATIE & TOEZICHTSRAPPORT

EXECUTIVE SUMMARY

PUBLIEKE VERSIE[1]

Referentienummer: CON19002

BETREFT: RAPPORT OVER DE VISITATIE BIJ EEN POLITIEZONE IN DE PROVINCIE OOST-VLAANDEREN DOOR HET CONTROLEORGAAN OP DE POLITIONELE INFORMATIE IN HET KADER VAN ZIJN TOEZICHTHOUDENDE EN CONTROLERENDE BEVOEGDHEID

[1] 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 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 geremedieerd aan een tekortkoming, enz ...

Voorwerp en opzet van het onderzoek

Op 20 juni 2019 heeft het Controleorgaan een omvangrijke visitatie uitgevoerd bij een lokale politiezone gelegen in de provincie Oost-Vlaanderen (Hierna PZ OVL). Met de visitatie wordt uitvoering gegeven aan het Strategisch Plan van het Controleorgaan waarbij wordt gestreefd om jaarlijks een aantal politiezones te bezoeken met het oog op de uitvoering van zijn controle- en onderzoeksbevoegdheden. Het toezicht bij de PZ OVL was een spontane visitatie. De visitatie was dus niet het gevolg van een (individuele) klacht of het gevolg van het bestaan van (concrete) aanwijzingen over het niet naleven van de wet- en regelgeving door de gevisiteerde PZ. Er werd geopteerd om een visitatie in de breedte uit te voeren. Dit betekent dat de visitatie betrekking had op meerdere thema's zonder al te diepgaand op de verschillende thema's in te gaan. Daarbij werd in het bijzonder aandacht besteed aan de toepassing van het juridisch kader inzake gegevensbescherming.

De visitatie omvatte vijf thema's:
1) Het gebruik van camera's
2) Controle op de kwaliteit van de gegevens en informatie in de ANG
3) Bijzondere gegevensbanken
4) Controlesystemen van het personeel
5) Informatieveiligheid: organisatie, beleid en ICT-beheer.

Onderzoeksbevindingen

De PZ OVL heeft zijn cameranetwerk over de jaren heen gaandeweg uitgebreid, waaronder het gebruik van vaste en mobiele ANPR-camera's. Op bepaalde wegen in de gemeente worden ANPR-camera's gebruikt met het oog op trajectcontrole. Daarbij rijst de vraag of op deze vorm van cameragebruik de bepalingen van de Wet op het Politieambt (WPA) inzake de voorwaarden en omstandigheden voor het gebruik van camera's van toepassing is. Het Controleorgaan is van oordeel dat het gebruik van ANPR-camera's voor trajectcontrole, die specifiek gericht is op snelheidscontrole, kadert binnen de toepassing van de wet van 16 maart 1968 betreffende de politie op het wegverkeer, waardoor het cameragebruik voor dit specifiek doeleinde buiten de toepassing van het cameragebruik in WPA valt. Deze vorm van cameragebruik valt echter buiten het opzet van de visitatie.

Opvallend was dat de PZ OVL niet meteen een antwoord kon geven op de vraag door wie deze ANPR-camera's zijn geplaatst en worden gebruikt. Uit het onderzoek blijkt dat de PZ OVL niet volgens de wettelijke regels op de hoogte werd gebracht van het plaatsen en gebruiken van deze camera's door de gemeente/stad. Bij ontstentenis van de mededeling ontslaat dit echter de korpschef niet van de plicht om uit eigen beweging na te gaan door wie camera's worden geplaatst en gebruikt en of daarbij de toepasselijke wetgeving wordt nageleefd. De PZ OVL maakt ook gebruik van niet-zichtbare ANPR-camera's. In dat geval wordt de camera gemonteerd in/op een anoniem politievoertuig. Deze vorm van cameragebruik moet evenwel voorafgaand aan het gebruik ervan aan het Controleorgaan aangegeven worden. Op het ogenblik van de visitatie was nog geen aangifte gedaan van het niet-zichtbaar gebruik van ANPR-camera's. Dat was ook bij het afsluiten van het rapport niet het geval.

Op het moment van de visitatie gebeurde de toegang tot de camerabeelden op basis van een algemene dienstlogin, wat niet in overeenstemming is met de wettelijke verplichtingen. Er werd geen gebruik gemaakt van een individualiseerbare toegang tot de ANPR-camerabeelden en er kon geen controle op het logbestand van de mobiele ANPR-camerabeelden uitgevoerd worden, wat nochtans wettelijk verplicht is. De PZ OVL beschikte ook niet over een (concreet) uitgewerkt toegangs- en gebruikersbeheer inzake cameragebruik. Deze tekortkomingen hadden kunnen voorkomen of geremedieerd worden indien de PZ een impact- en risicoanalyse of een 'DPIA'[2] voor (de verschillende vormen van) cameragebruik in de politiezone had opgemaakt. Dezelfde vaststelling geldt voor de oprichting van de lokale technische gegevensbanken voor de ANPR-beelden. Ook voor deze gegevensbank ontbreekt een impact- en risicoanalyse of een DPIA en het advies van de DPO. De politiezone beschikte evenmin over een register van cameragebruik.

[2] Data Protection Impact Analysis.

ANPR-camerabeelden kunnen aan registers gekoppeld worden. De lokale lijst van de PZ OVL voldoet echter niet aan alle wettelijke randvoorwaarden. Hoewel de lijst onderworpen is aan een hiërarchische toelating, zijn de beoordelingscriteria niet voorafgaand gedocumenteerd waardoor de proportionaliteit van de lijst niet kon worden beoordeeld. Noch wordt daarbij het advies van de DPO gevraagd.

Bij de verificatie van de logbestanden van de ANG bleek dat grotendeels geen reden van raadpleging werd ingevuld. Er is geen richtlijn (beleid) opgesteld en er wordt ook geen proactieve controle uitgevoerd. Het beheer van de toegangsprofielen wordt uitgevoerd conform de Ministeriële Omzendbrief MFO3. Een continue monitoring van de profielen en toegangen in real time in functie van de reële personeelsbezetting ontbreekt. De voeding vanuit de lokale toepassing naar het centrale niveau gebeurt op dagelijkse basis en de verwerpingen vanuit het centrale niveau worden op regelmatige basis behandeld. Bij de kwaliteitscontrole van de dossiers stelde zich in mindere mate een probleem. Het Controleorgaan stelde vast dat er geen enkele bijzondere gegevensbank in het register der verwerkingen is opgenomen.

De politiediensten verwerken ook persoonsgegevens voor niet-politionele doeleinden. In dat geval is naast de Wet Gegevensbescherming van 30 juli 2018 (WGB)[3] ook de AVG (GDPR) 2016/679[4] van toepassing. In dat verband maakt de PZ OVL gebruik van een systeem voor de registratie van vingerafdrukken van het personeel met het oog op tijdsregistratie. Naar het oordeel van het Controleorgaan ontbreekt daarvoor een wettelijke grondslag.

De PZ OVL heeft een functionaris voor de gegevensbescherming (DPO) aangewezen, die over de vereiste competenties beschikt en de functie voltijdse uitoefent, maar verdeeld over meerdere politiezones. Door het grote aantal politiezones die onder het werkveld van de DPO vallen, kan de DPO echter onmogelijk zijn opdrachten daadwerkelijk en efficiënt uitvoeren. Er werd vastgesteld dat de aangestelde DPO, gelet op de beperkte tijdsbesteding, niet ten gronde betrokken is bij de implementatie, het dagelijkse beheer en opvolging van het beleid inzake gegevensbescherming en informatieveiligheid. Daarnaast is het beleid inzake informatieveiligheid nog niet aangepast aan de actuele wet- en regelgeving. In dat verband konden een aantal richtlijnen (o.a. gebruik van Office 365 GPI en Sharepoint, e-mails en ICT devices) die in het dienstorder werden aangekondigd niet (ook niet in ontwerp) worden voorgelegd.

De aspecten van informatieveiligheid en gegevensbescherming kunnen op de agenda worden geplaatst van de wekelijkse vergadering van een managementteam (onder leiding van de korpschef). Aan deze vergaderingen wordt deelgenomen door de lokale coördinator/contactpersoon voor gegevensbescherming, maar niet systematisch door de DPO. De politiezone diende reeds onder de toepassing van het uitvoeringsbesluit van 6 december 2015 over een informatieveiligheidsplan te beschikken dat tijdens de visitatie niet beschikbaar was.

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

Het COC stelde vast dat er geen sterke netwerkauthenticatie vereist is voor toegang tot dit netwerk Er worden geen pro-actieve controles op de logbestanden uitgevoerd; dit gebeurt enkel op vraag. Rond het melden van gegevenslekken werd er nog geen procedure of sensibiliseringsactie gerealiseerd. Er is geen formeel ICT continuïteitsplan gedefinieerd binnen de ICT dienst. Desalniettemin zijn er acties ondernomen vanuit de ICT dienst van de politiezone om de beschikbaarheid van de digitale gegevens en de informatie-verwerkende faciliteiten te garanderen.

---

[3] Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (BS, 5 september 2018).

[4] 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 betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG.

Conclusie – aanbevelingen – corrigerende maatregelen

Conclusie

Een gering aantal aspecten van de gecontroleerde thema's blijken (volledig) in overeenstemming met de wetgeving. Aan de andere kant werden een aantal wettelijke tekortkomingen vastgesteld. Wat betreft de aspecten met een duidelijke dominantie op het vlak van gegevensbescherming blijkt dat de PZ OVL niet over de nodige specifieke kennis beschikt om op gepaste wijze antwoord te bieden op bepaalde gevoelige aangelegenheden. Niettegenstaande het overduidelijk engagement bij de aangestelde personeelsleden om op dat vlak de nodige inspanningen aan de dag te leggen, kan onvoldoende tijd worden vrijgemaakt om, naast de dagelijkse politietaken, gespecialiseerde opleiding te volgen. Deze vaststelling kan niet geheel worden opgevangen door de bijstand van de DPO zoals die in concreto kan geleverd worden.

Voorgaande algemene vaststelling weerspiegelt de omvang van de concrete vastgestelde tekortkomingen. Vooral op het domein van het gebruik van camerabewaking en de toepassing van het wettelijk kader met betrekking tot het gegevensbeschermingsrecht is nog een hele weg af te leggen. Hierbij geldt het gezegde: *bezint eer ge begint*. Doorgaans wordt door de politieoverheid een systeem aangekocht zonder het gebruik ervan voorafgaand kritisch te toetsen aan het toepasselijk wettelijk kader. Niet enkel de belangen van de politiedienst moeten in aanmerking worden genomen. Diverse aspecten moeten in rekening worden gebracht: de belangen van zowel de politie als de betrokkene (de burger dus, al dan niet inwoner van de politiezone), de ernst van de impact van het systeem op de persoonlijke levenssfeer van de betrokkene, het principe van *privacy by design*, gekoppeld aan een doorgedreven aandacht voor informatieveiligheid.

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

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

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

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

Aanbevelingen

1) Aanbeveling
Het is aanbevolen dat de korpschef in afwachting van een uitvoeringsbesluit ter zake een lokaal register van het cameragebruik aanlegt.

2) Aanbeveling
In het licht van de vastgestelde tekortkoming dringt het Controleorgaan er op aan dat een policy/beleid wordt opgesteld dat voorziet in een mechanisme waardoor periodiek en effectief controles worden uitgevoerd op (het monitoren van) eventuele (on)rechtmatige consultaties.

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

4) 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.

5) Aanbeveling
Het is van belang dat de korpschef dwingende richtlijnen opstelt waarin duidelijk onderscheid wordt gemaakt tussen de diverse aspecten die worden beoogd op het vlak van de toegang tot de virtuele omgeving. Zo moet de toegang tot het internet (zoekopdrachten, toegelaten en verboden websites) tijdens de diensturen worden onderscheiden van het gebruik van sociale media tijdens de diensturen voor persoonlijke doeleinden, enerzijds, en voor zover politionele informatie zou kunnen gedeeld worden, anderzijds. In een apart luik of afzonderlijk document wordt het gebruik van mobiele privétoestellen voor operationele doeleinden en het gebruik van professionele mobiele toestellen voor persoonlijke doeleinden (afzonderlijk) beschreven. Het is daarbij van belang dat het document duidelijk beschrijft wat toegelaten of verboden is, in welke omstandigheden en onder welke voorwaarden controle kan uitgevoerd worden, wat de gevolgen zijn wanneer inbreuken op het document worden vastgesteld en wat in dat verband de rechten van de betrokkene zijn.

6) Aanbeveling
Het wordt aanbevolen om de korpsrichtlijnen en procedures rond informatieveiligheid en gegevensbescherming verder te ontwikkelen en regelmatig te herzien. Het is hierbij belangrijk om deze richtlijnen te communiceren, te duiden en regelmatig te herhalen (door middel van bewustmakingscampagnes). Het is tevens van belang om blijvend via diverse informatiekanalen (mails/intranet/informatiesessies/vormingen/...) te voorzien in structurele en periodieke voorlichting rond aspecten van informatieveiligheid.

De medewerkers motiveren om veilig en correct om te gaan met persoonsgegevens en met de ICT-middelen door het ontwikkelen, toepassen en communiceren van goede praktijken ter zake wordt sterk aangemoedigd.

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

8) Aanbeveling
Het is aanbevolen de volgende actiepunten op te nemen in het informatieveiligheidsplan:

- Actualisering en verdere uitwerking van het beleid inzake informatieveiligheid en gegevensbescherming. Dit beleid moet regelmatig door het management gerevalueerd worden zodat het relevant blijft, in lijn met de realiteit.
- Maturiteitsmetingen, risico- en kwetsbaarheidsanalyses zijn belangrijke pijlers in het beveiligingsbeleid en dragen bij tot een optimale risico-gebaseerde informatieveiligheid. De tijdsbesteding van de DPO is ook een onderdeel van dit risicobeheer.

Het opzetten van formele overleg- en communicatieprocedures met alle betrokken partijen zodoende dat de DPO meer bij de werkzaamheden van de organisatie betrokken wordt en steeds over de nodige informatie beschikt voor de uitvoering van zijn opdracht die hem toevertrouwd werd is daarbij noodzakelijk.

9) 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 zijn uitgebreide toegangsrechten, in principe de sporen van zijn activiteiten wissen door bijvoorbeeld de systeemlogbestanden aan te passen of deze geheel te wissen.

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

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

11) Aanbeveling
Voor het toegelaten gebruik van mobiele gegevensdragers (usb sticks) is het aangewezen om extra veiligheidsmaatregen te voorzien: bijvoorbeeld het toepassen van encryptie en het opstellen en het regelmatig communiceren van instructies rond het veilig omgaan met mobiele gegevensdragers.

12) Aanbeveling
Het COC dringt er op aan om spoedig een structurele oplossing voor het monitoring van het lokale netwerk (admin/Wi-Fi) te voorzien en sterke netwerkauthenticatie te implementeren (met persoonlijk loggings) voor toegang tot het draadloze netwerk.

13) Aanbeveling
De politiezone dient een proces rond het melden van gegevenslekken uit te werken en te communiceren. Regelmatig sensibiliseren rond het thema van informatieveiligheidsincidenten, en in het bijzonder gegevenslekken, is sterk aangewezen.

14) Aanbeveling
De gebruikersprofielen voor toegang tot toepassingen en ICT-systemen dienen tevens actueel gehouden te worden conform de aanbeveling met betrekking tot de ANG.

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

Corrigerende Maatregelen opgelegd door het COC

Gelet op bovenstaande vaststellingen en aanbevelingen.

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

Gelast de PZ OVL:

a) om de toegang tot de camerabeelden in overeenstemming te brengen met artikel 25/7, § 1, derde lid, WPA, zodat de reden van de bevragingen geregistreerd wordt. Het bewijs van deze wetsconforme implementatie wordt binnen de zes maanden na datum van kennisname[5] van deze corrigerende maatregel aan het Controleorgaan overlegd;

b) binnen de 15 dagen na kennisname van huidig rapport aangifte te doen van het niet-zichtbaar gebruik van camera's;

c) aangifte te doen van de bijzondere gegevensbanken hetzij in REGPOL, hetzij in een eigen register van de verwerkingen en het Controleorgaan daarvan de bevestiging en het overzicht laten geworden binnen een termijn van 2 maand na kennisname van deze corrigerende maatregel van het Controleorgaan;

d) te bevestigen dat binnen een termijn van drie maanden na kennisname van deze corrigerende maatregel van het Controleorgaan geen gebruik meer zal gemaakt worden van de biometrische toegangscontrole, en na afloop van voormelde termijn derhalve enkel nog een alternatief systeem van toepassing zal zijn;

e) om een register van verwerkingen aan teleggen. Dit register wordt binnen de 2 maanden na kennisname van huidig rapport ter beschikking gesteld van het Controleorgaan;

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

Zeggen voor recht dat de aanvangsdatum van de corrigerende maatregelen en de datum van kennisname ervan bedoeld onder de littera a) tot en met f) moet begrepen worden als zijnde de datum van het overmaken van het huidig rapport van het Controleorgaan vermeerderd met twee dagen (zie ook voetnoot 1).

Aldus beslist door het Controleorgaan op de Politionele Informatie op 7 januari 2020.

* * * * * * * * *

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