VISITATIE- EN TOEZICHTSRAPPORT

EXECUTIVE SUMMARY

PUBLIEKE VERSIE

Referentienummer: CON19003

BETREFT: RAPPORT OVER DE VISITATIE BIJ EEN POLITIEZONE IN DE PROVINCIE NAMEN DOOR HET CONTROLEORGAAN OP DE POLITIONELE INFORMATIE IN HET KADER VAN ZIJN TOEZICHTHOUDENDE EN CONTROLERENDE BEVOEGDHEID[1]

[1] De publieke versie van een rapport van het Controleorgaan betekent dat deze versie niet of niet noodzakelijk alle elementen bevat die vermeld worden in het basisrapport dat aan 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 enzovoort.

VOORWERP EN OPZET VAN DE VISITATIE

Op 26 juni 2019 heeft het Controleorgaan (COC) een omvangrijke visitatie uitgevoerd bij een lokale politiezone in de provincie Namen (hierna "PZ PN" genoemd). 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 PN 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) De maatregelen inzake beveiliging van de informatie in het algemeen.
2) Het gebruik van camera's.
3) De toegang tot, de invoer en de kwaliteit van gegevens en informatie.
4) Bijzondere gegevensbanken.
5) De beveiliging en het beleid inzake ICT.

Onderzoeksbevindingen

Aan de hand van de antwoorden op de vragenlijst die het COC voorafgaand aan zijn visitatie hadden opgestuurd alsook van de waarnemingen binnen de PZ PN hebben we vastgesteld dat deze zone beschikt over een goede kennis van de verschillende wetgeving en de politionele richtlijnen inzake de verwerking van persoonsgegevens en het informatiebeheer.

We stelden vast dat de leiding van de PZ PN blijk geeft van een reële bereidheid om een actief beleid te voeren op het vlak van de gegevensbescherming en daartoe verschillende acties onderneemt. De PZ PN heeft begin 2018 al een DPO aangesteld en bood aan de betrokkene de kans verschillende opleidingen te volgen die specifiek verband houden met zijn functie.

De DPO van de PZ is nauw betrokken bij de uitvoering, het dagelijks beheer en de opvolging van het beleid inzake gegevensbescherming en informatieveiligheid.

Om op het vlak van de gegevensbescherming een stand van zaken op te stellen, voerde de DPO in de loop van 2018 een interne audit uit. De resultaten daarvan werden ter kennis gebracht van de leiding van de PZ om haar de kans te bieden de verschillende vastgestelde tekortkomingen te verhelpen.

Tijdens onze visitatie konden we vaststellen dat er als gevolg van deze audit vele initiatieven zijn genomen, met uitzondering van enkele punten die nog dienden te worden gerealiseerd. De PZ heeft binnen deze pijlers ook verschillende werkgroepen opgericht die de taak hebben de nieuwe richtlijnen in verband met de gegevensbescherming om te zetten. Aan de hand van verschillende concrete voorbeelden konden we vaststellen dat de PZ PN aan de oorsprong ligt van verschillende initiatieven en goede praktijken inzake toepassing van de AVG die worden gedeeld op het niveau van het arrondissement (provincie) Namen.

Vandaag bestaat er binnen de PZ PN niet langer een echt plan van informatiebeveiliging inzake ICT, daar dit plan werd opgenomen in het "Gegevensbeschermingsplan".

Er zijn bepaalde maatregelen uitgevoerd om garanties te bieden voor de integriteit, de vertrouwelijkheid en de continuïteit van de informatie en de informatiesystemen. Die maatregelen zijn echter niet het voorwerp van een structurele controle. Er wordt niet regelmatig overgegaan tot interne controles en zelfevaluaties op het vlak van ICT-beveiliging (bv. door middel van periodieke scans van de kwetsbaarheid overgaan tot proactieve detectie van de lacunes in de bescherming van de IT-systemen en de software). De voorbije jaren zijn er ook geen externe veiligheidsaudits gerealiseerd.

Bij de verificatie van de logbestanden van de ANG is gebleken dat de reden voor raadpleging in de meeste gevallen niet wordt vermeld. Er werd geen enkele (beleid) richtlijn uitgewerkt en er vinden geen proactieve controles plaats. De toegangsprofielen worden beheerd overeenkomstig de ministeriële rondzendbrief MFO3. Er is geen continue monitoring van de profielen of van de toegangen in reële tijd in functie van de reële personeelssterkte. De gegevensinvoer vanaf de lokale toepassing naar het centrale niveau vindt plaats op dagelijkse basis en de verwerpingen door het centrale niveau worden regelmatig behandeld.

De kwaliteitscontrole van de dossiers vormde een kleiner probleem, vooral op het vlak van de correcte en volledige uitvoering van de zgn. tryptiek (afnemen van vingerafdrukken, nemen van foto's en het opmaken van een individuele beschrijving).

Wat betreft de bijzondere gegevensbanken stelde het Controleorgaan vast dat die gegevensbanken (152) correct worden ingevoerd in het REGPOL-register. De toegankelijkheid van deze verschillende gegevensbanken steunt op het beginsel *need to know* (noodzaak op te weten). Deze verschillende gegevensbanken zijn toegankelijk via diverse software die niet altijd voldoende garanties biedt voor de traceerbaarheid en de controle van de toegang.

De PZ PN beschikt over een netwerk van 168 zichtbare camera's. In mei 2019 werd een impact- en risicoanalyse in verband daarmee gemaakt en doorgestuurd naar het COC. Deze verschillende camera's werden ook geregistreerd en geïnventariseerd in de IT-toepassing "Camelia".

De camerabeelden worden beheerd en verwerkt met specifieke software die is geïnstalleerd op een gescheiden netwerk. Deze software is slechts toegankelijk op een beperkt aantal computers, op basis van een persoonlijke login en volgens het toegekende profiel. De "live" beelden kunnen worden bekeken op alle computers waarop de specifieke software is geïnstalleerd; daarvoor dient men eerst in te loggen. Aanvragen om gearchiveerde beelden te bekijken worden ingediend door middel van een formulier dat wordt gegenereerd in ISLP[2]; de aanvrager moet zich identificeren en het voorwerp van zijn aanvraag nader beschrijven. De genomen maatregelen laten toe de aanvragen te traceren, maar de PZ voert momenteel geen proactieve controles uit.

In de loop van 2018 besliste de PZ om bodycams (op het lichaam gedragen camera's) aan te schaffen. Daartoe werd een testfase georganiseerd. Na afloop daarvan besliste de PZ om haar personeel uit te rusten met deze technologie. Een impact- en risicoanalyse met betrekking tot de bescherming van de persoonlijke levenssfeer werd uitgevoerd en gevalideerd op 23 november 2018 en werd vervolgens doorgestuurd naar het COC. Met het oog op transparantie en externe communicatie heeft de PZ PN de lokale bevolking via het gemeentelijk magazine geïnformeerd over het feit dat de personeelsleden van de PZ PN binnen afzienbare tijd zouden worden uitgerust met bodycams. Op 18 april 2019 werd een dienstnota met als titel "*Operationele richtlijnen inzake het gebruik van bodycams*" geschreven en verspreid onder het voltallige personeel van de PZ. Op het tijdstip van onze visitatie was het personeel van de PZ PN nog niet uitgerust met deze technologie wat het voor het COC niet mogelijk maakte om de invoering en het gebruik in de dagelijkse praktijk te verifiëren.

Ten tijde van de visitatie beschikte de PZ PN nog niet over een camera met ANPR-technologie en dus konden we het gebruik van deze technologie niet verifiëren. De PZ PN overweegt om in de nabije toekomst te gaan werken met de ANPR-technologie en in dit kader werd een impact- en risicoanalyse gemaakt op 3 juni 2019.

[2] Integrated System for the Local Police.

Op het ogenblik van onze visitatie maakte de PZ PN geen gebruik van niet zichtbare (heimelijke) camera's.

Tijdens onze visitatie hebben we vastgesteld dat sommige personeelsleden van de PZ de neiging hadden om persoonlijke apparaten en private berichtendiensten van het type *WhatsApp* te gebruiken. De PZ PN is zich bewust van deze praktijken, maar heeft in dit verband geen enkel beleid uitgewerkt, wetende dat dergelijke praktijken zullen verdwijnen met de implementatie van de applicatie "*Focus I-police*" tijdens de tweede helft van 2019.

Conclusie – aanbevelingen – corrigerende maatregelen

Conclusie

De visitatie van het COC heeft toegelaten vast te stellen dat de PZ PN sinds 2018 verschillende projecten, acties en goede praktijken heeft ontwikkeld op het vlak van gegevensbescherming en informatiebeveiliging.

Overigens ligt de PZ PN aan de oorsprong van verschillende initiatieven inzake gegevensbescherming op het niveau van het arrondissement Namen die tot doel hebben ervaringen en kennis ter zake uit te wisselen.

De bovenstaande algemene vaststelling weerspiegelt het streven van de PZ PN om een actief beleid te voeren op het vlak van informatieveiligheid. Tijdens de visitatie kon worden vastgesteld dat de PZ de vereiste specifieke kennis bezit om met een passend antwoord voor de dag te komen voor alle problemen in verband met de verschillende thema's in het domein van de bescherming van persoonsgegevens en de veiligheid van de informatie in het algemeen.

De visitatie heeft ook toegelaten vast te stellen dat de PZ PN de bedoeling heeft aan te sluiten bij een proces van modernisering van de politionele instrumenten en te streven naar de ontwikkeling van een grondiger digitalisering van het politiewerk. De PZ neemt immers deel aan heel wat projecten in haar hoedanigheid van proefzone. Het betreft meer bepaald de invoering van de applicatie *I-Police Focus*, het gebruik van bodycams en het gebruik van camera's met ANPR-technologie. Voor de laatste twee gevallen gaf de PZ voorrang aan een denkoefening, waarbij om te beginnen eerst een impact- en risicoanalyse op het vlak van de bescherming van de persoonlijke levenssfeer werd verricht om vervolgens een testfase te hebben teneinde verschillende soorten materieel te kunnen testen. Tegelijk voert de PZ een benchmarking bij andere eenheden die al gebruik maken van deze technologie.

Toch hebben we ter gelegenheid van de visitatie kunnen vaststellen dat de PZ PN moet blijven investeren in bepaalde domeinen waar enkele tekortkomingen werden vastgesteld, met als doel te streven naar uitmuntendheid in het beleid dat ze voert op het vlak van de bescherming van persoonsgegevens en informatieveiligheid.

Hoewel er op het niveau van het korps, sinds de visitatie, een aantal richtlijnen is opgesteld – andere worden momenteel nog geschreven – in verband met het thema van de toegang tot de verschillende gegevensbanken, moet de PZ PN aandacht blijven besteden aan deze problematiek.

Tevens moet de PZ PN haar initiatieven voortzetten wat betreft de fysieke beveiliging van haar lokalen en moet ze blijven investeren in dit domein.

Er wordt ook aanbevolen bijzondere aandacht te besteden aan de ICT-beveiliging, want de politiezone heeft geen algemeen ICT-veiligheidsplan. Een dergelijk plan zou toelaten de risico's te identificeren en te evalueren en vervolgens te bepalen welke passende beschermingsmaatregelen moeten worden genomen. Een dergelijke benadering op basis van het risico zou toelaten de genomen maatregelen te evalueren, te formaliseren en te documenteren.

Volgend op onze visitatie en onze opmerkingen liet de politiezone ons weten dat ze in de loop van 2020 een aantal initiatieven zou nemen op het vlak van informatiebeveiliging en dat ze ook periodieke tests BRP/BCM (*Disaster Recovery* / *Business Continuity*) zou uitvoeren.

Het past dan ook een reeks begeleidende aanbevelingen te formuleren die de doeltreffendheid en de efficiëntie van de PZ PN moeten helpen verbeteren inzake het beheer en de verwerking van persoonsgegevens in het bijzonder en van de politionele informatie in het algemeen.

De vastgestelde tekortkomingen ten aanzien van de vigerende wettelijke bepalingen nopen het Controleorgaan er echter toe **corrigerende maatregelen** te treffen waaraan de PZ PN binnen een welomschreven termijn gevolg zal moeten geven teneinde de situatie te regulariseren.

Aanbevelingen

1) Aanbeveling

Rekening houdende met de vastgestelde tekortkoming dringt het Controleorgaan erop aan dat er een beleid zou worden uitgewerkt inzake de onrechtmatige toegang tot de gegevensbanken. Dit beleid moet de vorm krijgen van een mechanisme van periodieke en effectieve controle (van de monitoring) van de eventuele (on)regelmatige raadplegingen, alsook van een richtlijn die de regels en de plichten voor het personeel in herinnering brengt inzake de raadpleging van de gegevensbanken (meer bepaald de traceerbaarheid van de geraadpleegde gegevens).

2) Aanbeveling

Er wordt aanbevolen om de richtlijnen van het korps en de procedures voor gegevensinvoer in de ANG nader te beschrijven en regelmatig te herzien. In deze context is het belangrijk deze richtlijnen mee te delen, ze toe te lichten en regelmatig in herinnering te brengen (via bewustmakingscampagnes). Bovendien is het belangrijk om – permanent en via verschillende informatiekanalen (e-mail / intranet / informatiesessies / opleidingen …) – structurele en periodieke instructies te verspreiden in verband met de verschillende aspecten betreffende de gegevensinvoer in de ANG.

Er wordt aanbevolen om de procedure van controle van de kwaliteit van de gegevensinvoer in de ANG te verbeteren, maar ook de controle op de gegevensinvoer te versterken op de verschillende hiërarchische niveaus.

3) Aanbeveling

Aan de PZ PN wordt aanbevolen zich ervan te vergewissen dat de ingebruikname van de applicatie "Focus" ertoe leidt dat er niet langer gebruik wordt gemaakt van persoonlijke apparaten noch van private berichtendiensten. Hoewel een richtlijn een kader zal creëren voor het gebruik van de toestellen die ter beschikking van de PZ PN worden gesteld, bevelen we het management aan om oog te hebben voor dit punt.

4) Aanbeveling

Er wordt aanbevolen om te voorzien in aanvullende veiligheidsmaatregelen voor het toegestane gebruik van mobiele gegevensdragers (USB-sleutels) alsook voor het gebruik van versleuteling, en om instructies uit te werken – en die regelmatig te verspreiden – voor een veilig gebruik van mobiele gegevensdragers.

5) Aanbeveling

Het Controleorgaan dringt er bij de politiezone op aan om in het kader van het operationeel beheer enkel het gebruik toe te staan van gebruikersaccounts op naam / individuele gebruikersaccounts.

Het gebruik van een generieke gebruikersaccount voor de administratie van het systeem moet zoveel mogelijk worden beperkt en is enkel toegestaan indien dit beantwoordt aan een technische vereiste. Gebruikers die beschikken over uitgebreide toegangsrechten, zoals de beheerders van systemen en applicaties (de "bevoorrechte gebruikers"), moeten ook hun dagelijkse taken uitvoeren in de systemen met behulp van een nominatief gebruikersaccount. Met gedeelde generieke accounts bestaat er een risico dat het niet mogelijk is te achterhalen wie verantwoordelijk is voor eventueel vastgesteld misbruik. Bovendien is een bevoorrechte gebruiker met kwaadwillig opzet in principe bij machte, dankzij zijn uitgebreide toegangsrechten, de sporen van zijn activiteiten te wissen door bijvoorbeeld de logbestanden van het systeem aan te passen of volledig te wissen.

6) Aanbeveling

De politiezone moet een procedure uitwerken en bekendmaken voor de aangifte van gegevenslekken. Er wordt ten zeerste aanbevolen om regelmatig te sensibiliseren in verband met incidenten op het vlak van informatiebeveiliging en inzonderheid van gegevenslekken.

7) Aanbeveling

Er wordt aanbevolen een ICT-noodplan op te stellen (DRP of "*Disaster Recovery Plan*") evenals een continuïteitsplan voor alle kritieke processen en essentiële informatiesystemen van de organisatie, alsook hun uitvoering op periodieke basis te testen. Een DRP voor ICT gaat veel verder dan alleen maar een *back-up* maken. Een dergelijk noodplan moet de organisatie voorbereiden op alle mogelijke rampen die een impact kunnen hebben op de informatie- en communicatiesystemen.

Door het COC opgelegde corrigerende maatregel(en)

Gelet op de bovenstaande vaststellingen en aanbevelingen,

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

Geeft bevel aan de PZ PN om:

a) een veiligheidsplan van de ICT-informatie op te maken. Dit informatieveiligheidsplan moet binnen de zes maanden vanaf de kennisname van het huidige rapport worden overgelegd aan het Controleorgaan;
b) aan het COC de resultaten te bezorgen van de tests *BRP/BCM* die zullen worden uitgevoerd en dit orgaan ook kennis te geven van de corrigerende maatregelen die zullen worden getroffen;
c) ten minste 4 keer per jaar willekeurige proactieve controles uit te voeren met betrekking tot onregelmatige raadplegingen van de gegevensbanken en het COC op de hoogte te houden van de resultaten.

Zegt voor recht dat de datum van inwerkingtreding van de corrigerende maatregelen en de datum van kennisname van die maatregelen zoals bedoeld in de punten a) tot en met c) moeten worden begrepen als de datum van doorgifte van het huidige rapport aan het Controleorgaan plus twee dagen.

Aldus beslist door het Controleorgaan op de Politionele Informatie op 27 januari 2020.

* * * * * * * * *