



CONTROLEORGaan OP DE POLITIEInFORMATIE

Uw referentie

Onze referentie

Bijlage(n)

Datum

DA250009

16.10.2025

Betreft: Advies betreffende het wetsontwerp houdende instemming met het akkoord tussen het Koninkrijk België en het Koninkrijk van Groot-Brittannië en Noord-Ierland betreffende de samenwerking op het gebied van rechtshandhaving

Het Controleorgaan op de politie informatie (hierna afgekort 'COC' of 'Controleorgaan').

Gelet op de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (BS, 5 september 2018, hierna afgekort als 'WVG') inzonderheid het artikel 59 §1, 2^e lid, artikel 71 en Titel VII, inzonderheid artikel 236.

Gelet op de wet van 3 december 2017 tot oprichting van een Gegevensbeschermingsautoriteit (hierna afgekort 'WOG').

Gelet op de wet van 5 augustus 1992 op het politieambt (hierna 'WPA').

Gelet op de *Law Enforcement Directive* 2016/680 van 27 april 2016 (hierna '*LED*').

Gelet op de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens.

Gelet op het verzoek van dhr. Bernard Quintin, minister van Veiligheid en Binnenlandse Zaken, belast met Beliris, op 21 augustus 2025 door het Controleorgaan ontvangen op elektronische drager / per brief, om een advies uit te brengen overeenkomstig voornoemde WVG.

Gelet op het verslag van de heer Ronny Saelens, lid-raadsheer *a.i.* van het Controleorgaan.

Brengt op 16 oktober 2025 het volgende advies uit.

I. Voorafgaande opmerking nopens de bevoegdheid van het Controleorgaan

1. In het licht van, respectievelijk, de toepassing en omzetting van de Verordening 2016/679¹ en de Richtlijn 2016/680² heeft de wetgever de taken en opdrachten van het Controleorgaan grondig gewijzigd. Artikel 4 §2, vierde lid, van de organieke wet van 3 december 2017 betreffende de oprichting van een Gegevensbeschermingsautoriteit (hierna afgekort 'WOG') bepaalt dat de competenties, taken en bevoegdheden als toezichthoudende autoriteit voorzien door de Verordening 2016/679 voor de politiediensten in de zin van artikel 2,2°, van de wet van 7 december 1998 tot organisatie van een geïntegreerde politie, gestructureerd op twee niveaus, worden uitgeoefend door het Controleorgaan. Het betekent onder meer dat het Controleorgaan ook bevoegd is wanneer politiediensten persoonsgegevens verwerken die buiten de opdrachten van bestuurlijke en gerechtelijke politie vallen, bijvoorbeeld in het kader van sociaaleconomische doeleinden of human resources verwerkingen. Het Controleorgaan moet geraadpleegd worden bij de voorbereiding van wetgeving of een regelgevende maatregel die verband houdt met de verwerking van persoonsgegevens door de politiediensten van de geïntegreerde politie (zie artikel 59 §1, 2^e lid en 236 §2 WVG, artikel 36.4 van de AVG en artikel 28.2 van de Richtlijn politie-justitie). Daarbij heeft het Controleorgaan de opdracht om te onderzoeken of de voorgenomen verwerkingsactiviteit door de politiediensten in overeenstemming is met de bepalingen van Titel 1 (voor de niet operationele verwerkingen)³ en 2 (voor de operationele verwerkingen) van de WVG⁴. Daarnaast heeft het COC ook een ambtshalve adviesopdracht voorzien in artikel 236 §2 WVG en een algemene voorlichtingsopdracht van het brede publiek, betrokkenen, verwerkingsverantwoordelijken en verwerkers in de materie van het privacy – en gegevensbeschermingsrecht voorzien in artikel 240 WVG.

2. Wat betreft derhalve in het bijzonder de verwerkingsactiviteiten in kader van de opdrachten van bestuurlijke en/of gerechtelijke politie brengt het Controleorgaan advies uit, hetzij uit eigen beweging, hetzij op verzoek van de Regering of van de Kamer van volksvertegenwoordigers, van een bestuurlijke of gerechtelijke overheid of van een politiedienst, inzake iedere aangelegenheid die betrekking heeft op het politionele informatiebeheer zoals geregeld in Afdeling 12 van Hoofdstuk 4 van de wet op het politieambt⁵.

¹ 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" (algemene verordening gegevensbescherming of 'AVG').

² 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 'Richtlijn Politie en Justitie' of 'Law Enforcement Directive (LED)').

³ Artikel 4 §2, 4^e lid WOG.

⁴ Artikel 71 §1, 3^e lid WVG.

⁵ Artikelen 59 §1, 2^e lid en 236 §2 WVG.

3. 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 de Passagiersinformatie-eenheid (hierna afgekort 'BELPIU') bedoeld in Hoofdstuk 7 van de wet van 25 december 2016 tevens belast met het toezicht op de toepassing van Titel 2 van de GBW en/of de verwerking van persoonsgegevens zoals bedoeld in de artikelen 44/1 tot 44/11/13 van de wet op het politieambt en/of elke andere opdracht die haar krachtens of door andere wetten wordt verleend⁶.

4. 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 BELPIU in fiscale materies.

5. Het COC is tot slot ook belast, in het kader van de dataretentie wetgeving, op grond van artikel 126/3 §1, 8^e lid van de wet van 13 juni 2005 betreffende de elektronische communicatie (hierna afgekort 'WEC'), 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), met de 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 bij titel 7 van de wet van 30 juli 2018. Het is daarnaast ook nog belast, in toepassing van artikel 42 §3, 2^{de} en 3^{de} 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.

6. Het Controleorgaan is bevoegd om advies te verlenen over aspecten met betrekking tot de verwerking van informatie en persoonsgegevens en de bescherming van het privéleven door de verwerking van persoonsgegevens voor zover deze betrekking hebben op of in verband staan met de operationele en niet-operationele werking van de politiediensten en/of het personeel van de geïntegreerde politie (hierna 'GPI'⁷) en/of voor zover de voor advies voorgelegde ontwerp tekst een impact heeft op de politieke informatiehuishouding in het algemeen.

⁶ Artikel 71 §1, derde lid *juncto* 236 § 3 WVG.

⁷ Geïntegreerde politie – Police Intégrée.

7. Het Controleorgaan is daarnaast niet enkel een gegevensbeschermingsautoriteit maar een toezichthouder die evenzeer wettelijk belast is met de legaliteit, efficiëntie, effectiviteit en economie van de politionele informatiehuishouding⁸.

II. Voorwerp van de aanvraag

8. De minister van Veiligheid en Binnenlandse Zaken maakte op 21 augustus 2025 een verzoek tot advies aan het COC over met betrekking tot een wetsontwerp houdende instemming met een bilateraal akkoord tussen het Koninkrijk België en het Koninkrijk van Groot-Brittannië en Noord-Ierland betreffende de samenwerking op het gebied van rechtshandhaving (hierna 'het ontwerpakkoord').

9. De opstellers van het ontwerpakkoord onderstrepen het gemeenschappelijk belang van beide landen op het vlak van veiligheid, dat zich vertaalt in grensoverschrijdende politionele samenwerking. Deze samenwerking krijgt meer bepaald de vorm van intensieve informatie-uitwisseling tussen de politiediensten van beide landen alsook van de oprichting van samenwerkingsstructuren, inzonderheid voor de uitvoering van grensoverschrijdende politionele opdrachten. Bovendien zijn de mogelijkheden voor politionele samenwerking op het gebied van veiligheid tussen beide landen gevoelig kleiner geworden sinds de beslissing van het Verenigd Koninkrijk in 2020 om uit de Europese Unie te stappen. Uit de memorie van toelichting blijkt dat de opstellers van het ontwerpakkoord inspiratie hebben gehaald uit het Benelux-politieverdrag van 23 juli 2018⁹.

In het begeleidend schrijven van de minister van Binnenlandse Zaken bij het ontwerpakkoord wordt benadrukt dat het gaat om een ontwerp van '*technisch*' akkoord; dit betekent dat er nog bepaalde wijzigingen kunnen worden aangebracht. Het advies van het COC heeft dus enkel betrekking op de versie van het ontwerpakkoord zoals die aan het COC werd overgelegd.

III. Analyse van de aanvraag

10. Om te beginnen wenst het COC de aandacht te vestigen op de kwaliteit en de nauwgezetheid wat betreft de formulering met betrekking tot de gegevensbeschermingsrechtelijke aspecten in het samenwerkingsakkoord, waarbij heel bijzondere aandacht wordt besteed aan het geheel van definities die een duidelijk kader bieden dat op alle punten identiek is aan het Belgische rechtskader ter zake.

Tevens legt het COC de nadruk op de positieve aanwezigheid van een wetsbepaling die specifiek betrekking heeft op de creatie van een rechtsgrondslag en van garanties in het kader van de *ANPR*-

⁸ Activiteitenverslag 2021, www.controleorgaan.be, randnummers 3, 52 en in het bijzonder 71: "Het COC heeft echter allerminst alleen oog voor dataprotectie; het heeft evenzeer veel aandacht en is bevoegd voor alle andere operationele aspecten van de politionele informatiehuishouding"; artikel 71 §1 WVG.

⁹ Verdrag tussen het Koninkrijk België, het Groothertogdom Luxemburg en het Koninkrijk der Nederlanden inzake politiesamenwerking.

informatie-uitwisseling¹⁰; op die manier wordt er meer rechtszekerheid geboden wat betreft de doorgifte van geautomatiseerde gegevens.

A. Algemene opmerkingen

1. Verdere doorgiften naar derde landen of internationale organisaties

11. Overeenkomstig de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens kan een doorgifte van persoonsgegevens aan een land buiten de Europese Unie of een internationale organisatie meer bepaald plaatsvinden wanneer "*de Europese Commissie bij adequaatheidsbesluit bepaald heeft dat het land, een gebied of één of meerdere nader bepaalde sectoren in dat land, of de internationale organisatie in kwestie een passend beschermingsniveau waarborgt*"¹¹. De criteria die het passende beschermingsniveau definiëren zijn terug te vinden in Richtlijn 2016/680 ('Richtlijn Politie – Justitie' of *LED*)¹² en bepalen dat de Commissie inzonderheid rekening houdt met de volgende elementen:

- de rechtstaat, de eerbiediging van de mensenrechten en de fundamentele vrijheden, de toepasselijke algemene en sectorale wetgeving, (...);
- het bestaan en het effectief functioneren van een of meer onafhankelijke toezichthoudende autoriteiten in het derde land of waaraan een internationale organisatie is onderworpen, welke tot taak heeft of hebben de naleving van de gegevensbeschermingsregels te verzekeren en deze te handhaven, (...); en
- de internationale verbintenissen die het derde land of de internationale organisatie in kwestie heeft aangegaan, of andere verplichtingen die voortvloeien uit juridisch bindende overeenkomsten of instrumenten, alsmede uit de deelname van dat derde land of die internationale organisatie aan multilaterale of regionale regelingen, in het bijzonder met betrekking tot de bescherming van persoonsgegevens.

12. Hoewel er wat betreft de wetgeving inzake de bescherming van persoonsgegevens op het gebied van de rechtshandhaving in het Verenigd Koninkrijk globaal gezien een behoud van het beschermingsniveau wordt waargenomen sinds de 'Brexit', valt op te merken dat het Verenigd Koninkrijk bepaalde wijzigingen heeft doorgevoerd wat betreft de goedkeuring van doorgiften tegen passende waarborgen, in het Engels '*adequacy regulations*' genoemd, die voorheen waren opgenomen in artikel 74A van de *UK Data Protection Act* (hierna '*UK DPA*').

¹⁰ *Automatic Number Plate Recognition*.

¹¹ Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, artikel 67.

¹² 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, artikel 36(2).

Deze bepalingen werden inderdaad geherformuleerd en in plaats van de doorgifte afhankelijk te maken van een '*passend beschermingsniveau*' zoals vandaag het geval is in België¹³ en zoals gedefinieerd in de Richtlijn Politie – Justitie (*LED*), bepalen ze voortaan dat een doorgifte mogelijk is indien de beschermingsvoorwaarden voor burgers niet '*materieel minder(waardig)*' zijn dan die welke van toepassing zijn in het Verenigd Koninkrijk¹⁴.

Zo blijkt dat er minder elementen in aanmerking moeten worden genomen in het kader van de beoordeling zoals bedoeld in artikel 74AB(2) *UK DPA*, alsook dat er criteria verdwenen zijn die voorheen waren opgenomen in het inmiddels geschrapte artikel 74A(4) *UK DPA* en die op alle punten overeenkwamen met de criteria die toelaten de '*adequaatheid van het beschermingsniveau*' te beoordelen zoals bedoeld in artikel 36(3) *LED*.

13. Voor het overige stellen we toch vast dat, zoals bepaald in artikel 14 van het samenwerkingsakkoord, het voorafgaand akkoord van het land dat de persoonsgegevens doorgeeft vereist is voor elke verdere doorgifte door het land dat de informatie ontvangt. Deze voorwaarde zou erop neerkomen dat de beslissing tot verdere doorgifte zou berusten bij de Belgische politiediensten in hun hoedanigheid van overheid die de informatie doorgeeft. Het blijft echter essentieel om deze wetswijziging te vermelden, daar ze impliceert dat het beschermingsniveau van de burgers afneemt wanneer de Britse politiediensten hun persoonsgegevens verwerken.

14. De memorie van toelichting onderstreept het belang van een passend niveau van bescherming van de persoonsgegevens in het derde land, in dit geval dus het Verenigd Koninkrijk. Het verdient dus aanbeveling om in de inleiding van het ontwerpakkoord de toepassing van de *LED* op te nemen, ten minste met betrekking tot België, wat betreft de doorgifte van persoonsgegevens aan het Verenigd Koninkrijk.

15. De nadere regels voor informatie-uitwisseling, met inbegrip van persoonsgegevens, enerzijds en de kanalen voor informatie-uitwisseling anderzijds maken respectievelijk het voorwerp uit van de artikelen 7 en 10 van het ontwerp, terwijl de nadere regels voor uitwisseling van *ANPR*-gegevens¹⁵ specifiek worden vastgelegd in artikel 11 van het ontwerpakkoord.

16. Wat betreft de modaliteiten van gegevensuitwisseling kan dergelijke uitwisseling ook '*spontaneously*' (i.e. ambtshalve) plaatsvinden tussen, onder andere, de '*competent services*' (de bevoegde diensten) zoals bedoeld in artikel 10, paragraaf 4, van het ontwerp, "*in cases where there are reasons to believe such information is necessary (...)*"¹⁶. Volgens het COC moet deze bepaling worden geïnterpreteerd als **een doorgifte geval per geval** van persoonsgegevens, wat impliceert dat

¹³ Artikel 67 WVG.

¹⁴ UK Data Protection Act of 23 May 2018, section 74AB.

¹⁵ *Automatic Number Plate Recognition*.

¹⁶ "*In de gevallen waarin er redenen zijn om aan te nemen dat die informatie noodzakelijk is*" (vrij vertaald).

een *spontane* uitwisseling **niet kan bestaan in een eenzijdige, algemene en stelselmatige doorgifte van persoonsgegevens**. Op dit niveau van uitwisseling bestaat er immers niet de minste controle door het centrale contactpunt (*SPOC*)¹⁷ zoals bedoeld in artikel 10, paragraaf 1, van het ontwerpakkoord. Dit risico moet ten minste worden vermeld en gerechtvaardigd in de memorie van toelichting.

17. Wat betreft de wijze van doorgifte van *ANPR*-gegevens voorziet het ontwerp artikel 11 in specifieke regelgeving wegens de ernst van het risico voor de bescherming van de persoonlijke levenssfeer in verband met de verwerking (doorgifte) van deze persoonsgegevens. In tegenstelling met andere politionele gegevens die mogen worden uitgewisseld (cf. *supra*), worden deze gegevens uitgewisseld via de *SPOC* zoals genoemd in artikel 10, paragraaf 1, van het ontwerp. Artikel 11 §3, van het ontwerp luidt als volgt:

*"Reference data as defined in paragraph 1 of this article shall be transferred between central contact points as laid down in paragraph 1 of article 10 of this Agreement."*¹⁸.

Om te vermijden dat de draagwijdte van deze bepaling op minder strikte wijze wordt geïnterpreteerd, wordt aanbevolen om het woord '*only*' in te voegen tussen de woorden '*shall*' en '*be*' alsook om in de memorie van toelichting nader vast te stellen dat deze bepaling dus de toepassing uitsluit van de afwijkingen waarin artikel 10 §3 en §4 van het ontwerp voorziet.

2. Recht op toegang

18. In het kader van dit ontwerp van samenwerkingsakkoord regelt artikel 12 §3, het recht op informatie, op toegang, op rechtzetting en op het wissen van persoonsgegevens "*in accordance with the legal framework applicable*"¹⁹, wat het COC interpreteert als "*overeenkomstig het nationale recht*". In overeenstemming met artikel 12 §3 b) van het ontwerp is elke verdragsluitende Staat verplicht om zich ervan te vergewissen dat elke burger die heeft vastgesteld dat de eigen persoonsgegevens werden verwerkt volgens de bepalingen van dit akkoord, de mogelijkheid heeft – rechtstreeks of onrechtstreeks (i.e. via een toezichthoudende autoriteit zoals het COC) – om zijn rechten uit te oefenen, meer bepaald om de bevestiging te krijgen van een eventuele verwerking van persoonsgegevens door een rechtshandhavingsautoriteit in een van de Staten die dit akkoord sluiten en om toegang tot die gegevens te krijgen in een begrijpelijke vorm.

19. Wat betreft het recht op toegang van burgers met betrekking tot de persoonsgegevens die de rechtshandhavingsautoriteiten verwerken, zoals dat recht in België wordt uitgeoefend, worden de verificaties verricht door het COC in zijn hoedanigheid van toezichthoudende autoriteit middels een

¹⁷ *Single Point Of Contact*.

¹⁸ *"De referentiegegevens zoals gedefinieerd in paragraaf 1 van dit artikel worden doorgegeven tussen de centrale contactpunten overeenkomstig paragraaf 1 van artikel 10 van dit akkoord."* (vrij vertaald).

¹⁹ *"Overeenkomstig het toepasselijke rechtskader"* (vrij vertaald).

systeem van onrechtstreekse toegang. De mogelijkheden om de burgers inhoudelijk te informeren zijn zeer beperkt. Het COC is gehouden om elk verzoek tot toegang af te sluiten met de volgende standaardzin: *"De nodige verificaties werden verricht."* Op grond van artikel 42 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens is het Controleorgaan nog steeds niet gemachtigd om de inhoud van de verwerkte gegevens mee te delen, noch om aangebrachte wijzigingen (of juist geen) te motiveren.

20. De wetgeving inzake gegevensbescherming in het Verenigd Koninkrijk voorziet van haar kant in een systeem van (rechtstreekse) toegang wat betreft de persoonsgegevens dat verenigbaar is met artikel 12 §3 b) van het samenwerkingsakkoord. Het Britse recht bepaalt dat een betrokkene het recht heeft om van de verwerkingsverantwoordelijke de bevestiging te krijgen dat persoonsgegevens die op hem of haar betrekking hebben, al dan niet het voorwerp uitmaken van verwerking; zo dat het geval is, heeft de betrokkene recht op toegang wat betreft de persoonsgegevens en de informatie²⁰.

21. In deze context, en in de mate waarin de beperking zoals bedoeld in artikel 42 WVG – zoals hierboven nader uiteengezet – niet in aanmerking zou worden genomen door het Verenigd Koninkrijk, zou er sprake kunnen zijn van een onverenigbaarheid wat betreft de verwerking van het recht op toegang via artikel 12 van het ontwerpakkoord. Er zouden zich twee mogelijke scenario's kunnen voordoen die een vermelding vereisen in het huidige advies.

- Ten eerste, in de hypothese van een informatiestroom van België naar het Verenigd Koninkrijk, zou een burger vaststellen dat de inhoud van zijn recht op toegang wordt beperkt door de tekst van artikel 42 WVG, maar zou hij daarentegen potentieel alle of een deel van de informatie in het Verenigd Koninkrijk wél kunnen verkrijgen. Dit zou kunnen leiden tot een probleem inzake vertrouwelijkheid van de informatie die de Belgische politiediensten verstrekken. In dit geval zou het noodzakelijk zijn om te voorzien in een mechanisme dat de bevoegde Britse diensten ertoe verplicht worden om zich tot België te richten teneinde te weten welke informatie mag worden bekendgemaakt.

- In een tweede hypothese van een informatiestroom vanwege de Britse diensten naar België zou de burger volledige of gedeeltelijke inzage krijgen van zijn persoonsgegevens in het Verenigd Koninkrijk, maar zou hij vaststellen dat zijn identieke verzoek in België wordt beperkt als gevolg van de in artikel 42 WVG opgelegde limieten. Dit vormt in se geen probleem, maar het zal natuurlijk incoherent voorkomen.

B. Bijzondere opmerkingen

22. Vervolgens wenst het Controleorgaan nog enkele bijzondere vaststellingen te vermelden die werden gedaan bij de lezing van het ontwerp van samenwerkingsakkoord.

²⁰ UK Data Protection Act of 23 May 2018, section 45.

23. Ontwerpartikel 2 §1 definieert het materiële toepassingsgebied van het ontwerpakkoord. Het luidt als volgt:

*"The Parties undertake to assist each other in the performance of their respective law enforcement tasks, in accordance with the provisions of this Agreement."*²¹.

Volgens het COC is deze doelstelling wel bijzonder vaag. Daar de opstellers van het ontwerpakkoord zich voornamelijk baseren op het hierboven genoemde Benelux-politieverdrag, wordt aanbevolen om de formulering van het artikel daarvan deels over te nemen; artikel 2 §1 zou dan als volgt worden aangevuld:

*"a) preventie, onderzoek en opsporing van strafbare feiten en
b) handhaving van de openbare orde en veiligheid."*

In verband hiermee worden voorbeeld van subdoelstellingen opgenomen in ontwerpartikel 2. b).

24. Het ontwerpakkoord voorziet in artikel 12 §10 in een principieel verbod op uitsluitend geautomatiseerde besluitvorming, tenzij het nationale recht dergelijke besluitvorming uitdrukkelijk toestaat. In tegenstelling tot het ontwerpartikel vermeldt de memorie van toelichting bij dit artikel *"of profiling"*. Dit principieel verbod moet echter ook uitdrukkelijk worden opgenomen in het ontwerpartikel, daar niet elke geautomatiseerde beslissing *ipso facto* en/of *de jure* ook profilering impliceert. In dit verband valt op te merken dat de wet op het politieambt geen regels bevat voor het gebruik van politonele gegevens voor doeleinden van profilering, noch voor de problematiek van geautomatiseerde beslissingen.

25. Vervolgens neemt het Controleorgaan, wat betreft de beveiliging van de informatie²², nota van de noodzaak om technische en organisatorische maatregelen te nemen die zijn ontworpen voor de bescherming tegen niet-toegestane of onwettige verwerkingen, accidenteel verlies, vernietiging van of schade aan informatie die op basis van het akkoord wordt uitgewisseld.

Er zou eventueel kunnen worden bepaald dat de te nemen technische en organisatorische maatregelen *'passend'* moeten zijn met als doel een drempel voor implementatie van minimale maatregelen in de informatiebeveiliging vast te stellen.

26. Het ontwerpartikel 16 van het akkoord voorziet in de mogelijkheid voor de operationele leden van de politiediensten van beide verdragsluitende Staten om hun informatie uit te wisselen krachtens een mondelinge toelating, ondanks het systeem van 'voorafgaande schriftelijke goedkeuring' dat meermaals wordt vermeld in het ontwerp²³. Er wordt bepaald dat deze mogelijkheid wordt beperkt tot sommige precieze gevallen en wordt gevolgd door een schriftelijke bevestiging. Vanuit het oogpunt van bescherming van de gedeelde informatie zou de tekst er echter baat bij kunnen hebben dat er wordt

²¹ *"De partijen verbinden zich ertoe elkaar wederzijds bijstand te verlenen in de uitvoering van hun respectieve taken op het vlak van repressie, in overeenstemming met de bepalingen van het huidige akkoord."* (vrij vertaald).

²² Art. 7b §1 van het samenwerkingsakkoord.

²³ Art. 14 en art. 15 van het samenwerkingsakkoord.

toegevoegd dat de schriftelijke bevestiging op de mondelinge toelating moet volgen "zonder ongerechtvaardigde vertraging"²⁴ teneinde de nadruk te leggen op het belang van de schriftelijke aard van de akkoorden voor doorgifte van operationele informatie tussen de bevoegde diensten.

27. Tot slot, en hoewel in de initiële e-mail met het verzoek inderdaad wordt uiteengezet dat de tekst van het akkoord nog wat moet worden bijgewerkt, merkt het COC op dat sommige begrippen er baat bij zouden hebben te worden verduidelijkt. We vermelden bijvoorbeeld §4 lid 2 en §5 lid 4 van artikel 12, waar wordt verwezen naar de mogelijkheid om te weigeren potentieel verkeerde informatie te schrappen die een burger zou betwisten indien de waarachtigheid van deze informatie niet kan worden bevestigd. Er wordt dan voorgesteld om de toegang tot deze potentieel verkeerde informatie te 'markeren' of op een andere wijze te beperken. Er wordt niet nader vermeld wat het gevolg is van het feit potentieel verkeerde informatie te 'markeren'. Naar het voorbeeld van het rechtskader waarin hiervoor wordt voorzien in de *LED*, wordt er enkel bepaald dat de informatie moet worden beperkt²⁵. Het lijkt dus verstandig om de draagwijdte van het artikel te beperken tot "*de persoonsgegevens beperken*" of te definiëren wat wordt verstaan onder het feit de informatie te 'markeren'; de Europese wetgeving ter zake voorziet niet in deze tweede mogelijkheid en definieert ze ook niet.

OM DEZE REDENEN,

Het Controleorgaan op de Politie Informatie,

verzoekt de aanvrager rekening te houden met de hogervermelde opmerkingen.

Advies goedgekeurd door het Controleorgaan op de Politie Informatie op 16 oktober 2025.

Voor het Controleorgaan,

De Voorzitter *a.i.*,

Frank SCHUERMANS (GET)

²⁴ In het Engels "*without undue delay*".

²⁵ Richtlijn *LED* (EU) 2016/680, considerans 47 en art. 16.