CONTROLEORGAAN OP DE POLITIONELE INFORMATIE

Uw referentie	Onze referentie	Bijlage(n)	Datum
	DD220019		13.02.2024

Betreft: Advies uit eigen beweging betreffende de verwerking van persoonsgegevens van personeelsleden van een politie-entiteit met het oog op het beheer van de toegang tot de bewapening – Verwerking van vingerafdrukken van personeelsleden voor hetzelfde doel.

Het Controleorgaan op de politionele informatie (hierna 'het Controleorgaan' of het 'COC').

Gelet op de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (B.S. van 5 september 2018, hierna afgekort als "wet betreffende de gegevensbescherming" of "WVG"), inzonderheid artikel 59, §1, 2de lid, artikel 71 en Titel VII, inzonderheid artikel 236.

Gelet op de wet van 5 augustus 1992 op het politieambt (hierna afgekort als "WPA"), inzonderheid de artikelen 3, 6° en 25/1 tot en met 25/7.

Gelet op artikel 236, §2, eerste lid van de WVG, dat voorziet in de mogelijkheid, voor het Controleorgaan, om uit eigen beweging adviezen uit te brengen.

Gelet op artikel 237 van de WVG.

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

Brengt op 13.02.2024 het volgend advies uit.

Inhoudsopgave

VOORAFGAANDE OPMERKING NOPENS DE BEVOEGDHEID VAN HET CONTROLEORGAAN

1. In het licht van, respectievelijk, de toepassing en de omzetting van de Verordening 2016/679[1] en de Richtlijn 2016/680[2] 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 tot oprichting van de Gegevensbeschermingsautoriteit (hierna "WOG") bepaalt dat de competenties, taken en bevoegdheden als toezichthoudende autoriteit bedoeld 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. Dat betekent met name dat het Controleorgaan ook bevoegd is wanneer politiediensten persoonsgegevens verwerken die niet onder de opdrachten van bestuurlijke en gerechtelijke politie vallen, bijvoorbeeld in het kader van sociaaleconomische doeleinden of HR-verwerkingen. Het Controleorgaan moet worden geraadpleegd in het kader van de voorbereiding van wetgeving of een regelgevende maatregel betreffende de verwerking van persoonsgegevens door de politiediensten van de geïntegreerde politie (zie artikelen 59, §1, 2de lid en 236, §2, van de WVG, artikel 36.4 van de AVG en artikel 28.2 van de Richtlijn Politie-Justitie). In dit kader heeft het Controleorgaan als opdracht om na te gaan of de door de politiediensten beoogde verwerkingsactiviteit in overeenstemming is met de bepalingen van Titel 1 (voor de niet-operationele verwerkingen)[3] en van Titel 2 (voor de operationele verwerkingen) van de WVG[4]. Bovendien heeft het COC ook een opdracht van advies uit eigen beweging, zoals bepaald in artikel 236, §2, van de WVG, en een opdracht van algemene informatieverstrekking aan het grote publiek, de betrokkenen, de verwerkingsverantwoordelijken en de verwerkers op het gebied van het recht op bescherming van de persoonlijke levenssfeer en gegevensbescherming, zoals bepaald in artikel 240 van de WVG.

2. Met betrekking tot in het bijzonder de verwerkingsactiviteiten in het kader van de opdrachten van bestuurlijke en/of gerechtelijke politie brengt het Controleorgaan uit eigen beweging of op verzoek van de regering of de Kamer van Volksvertegenwoordigers, een bestuurlijke of gerechtelijke autoriteit of een politiedienst advies uit over elke aangelegenheid die verband houdt met het beheer van politionele informatie, zoals bepaald in afdeling 12 van hoofdstuk 4 van de wet op het politieambt[5].

---

[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 (hierna de 'Algemene Verordening Gegevensbescherming' of 'AVG' genoemd).
[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 de "Richtlijn Politie en Justitie" of *Law Enforcement Directive* (LED) genoemd).
[3] Artikel 4 §2, 4de lid van de WVG.
[4] Artikel 71 §1, 3de lid van de WVG.
[5] Artikelen 59 §1, 2de lid en 236 §2, van de 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 "BEL-PIU") bedoeld in Hoofdstuk 7 van de wet van 25 december 2016 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 44/11/13 van de wet op het politieambt en/of elke andere opdracht die krachtens of door andere wetten aan het Controleorgaan wordt verleend[6].

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 passagiersgegevens" ten aanzien van de Dienst Geschillen van de Algemene Administratie van Douane en Accijnzen bevoegd in het kader van de vorderingen gericht aan de BEL-PIU in fiscale materies.

5. Tot slot is het Controleorgaan, in het kader van de wetgeving betreffende het bijhouden van de gegevens en krachtens artikel 126/3, §1, lid 8, van de wet van 13 juni 2005 betreffende de elektronische communicatie (hierna "de 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 (B.S. van 8 augustus 2022), ook belast met de validering (of niet) van de statistieken betreffende het aantal strafbare feiten en de opslagperiode voor elk gerechtelijk arrondissement en elke politiezone, i.e. een materie waarin het alle bevoegdheden uitoefent die aan dit orgaan werden verleend door Titel 7 van de wet van 30 juli 2018. Bij toepassing van artikel 42, §3, lid 2 en lid 3, van de WPA is het ook belast met de controle van de verzoeken van de Cel Vermiste Personen van de federale politie met het oog op de consultatie van de gegevens betreffende de elektronische communicatie waarbij de verdwenen persoon betrokken is.

6. Het Controleorgaan is bevoegd om adviezen te verlenen over de aspecten die betrekking hebben op de verwerking van informatie en van persoonsgegevens en op de bescherming van de persoonlijke levenssfeer door de verwerking van persoonsgegevens voor zover er een verband bestaat met de operationele en de niet-operationele werking van de politiediensten en/of met het personeel van de geïntegreerde politie (hierna "de GPI[7]") en/of voor zover het voor advies ingediende ontwerp van tekst een impact heeft op het beheer van de politie-informatie in het algemeen.

[6] Artikel 71 §1, derde lid *juncto* artikel 236 §3, van de WVG.
[7] **G**eïntegreerde politie – **P**olice **I**ntégrée.

7. Bovendien is het Controleorgaan niet alleen een gegevensbeschermingsautoriteit maar ook een toezichthoudende autoriteit die wettelijk belast is met de controle op de wettelijkheid, de doeltreffendheid, de efficiëntie en de economie van het beheer van politionele informatie[8].

VOORWERP EN CONTEXT VAN HET ADVIES

8. In het kader van de uitoefening van zijn opdrachten heeft het Controleorgaan veel informatieverzoeken ontvangen met betrekking tot de verwerking van vingerafdrukken van personeelsleden met het oog op het beheer van de toegang tot specifieke lokalen in politiegebouwen.

9. Gelet op de groeiende interesse van sommige politie-entiteiten voor de verwerking van biometrische gegevens – meer bepaald vingerafdrukken – van personeelsleden in het kader van beleid van toegangsbeheer alsook rekening houdend met de bijzonder gevoelige aard van biometrische gegevens heeft het Controleorgaan beslist om een advies uit eigen beweging op te stellen.

10. Dit advies heeft betrekking op de kwestie van de wettelijkheid van de verwerking van vingerafdrukken van personeelsleden van een politie-entiteit voor het beheer van de toegang tot bewapening.

Duidelijkheidshalve wijst het Controleorgaan erop dat enkel de term "bewapening" zal worden gebruikt om te verwijzen naar alle – individuele, collectieve of bijzondere – wapens, met inbegrip van neutraliserende middelen, waarmee de personeelsleden van de geïntegreerde politie zijn uitgerust alsook hun munitie en accessoires zoals bedoeld in artikel 1 van het Koninklijk besluit van 3 juni 2007 "*betreffende de bewapening van de geïntegreerde politie, gestructureerd op twee niveaus, alsook de bewapening van de leden van de Diensten Enquêtes bij de Vaste Comités P en I en van het personeel van de Algemene Inspectie van de federale politie en van de lokale politie*"[9].

11. Het huidige advies blijft strikt beperkt tot de problematiek van de verwerking van persoonsgegevens (vingerafdrukken) van leden van de politiediensten in het kader van een intern beleid voor beheer van de toegang tot bewapening (in bezit nemen, terugbrengen en opslaan van wapens). We onderzoeken dit onderwerp op twee fasen: enerzijds de wettelijkheid van de verwerking van persoonsgegevens met het oog op het beheer van de toegang tot bewapening, anderzijds de

[8] Activiteitenverslag 2021, www.controleorgaan.be, zie de punten 3 en 52 en inzonderheid punt 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 en die van de andere gecontroleerde diensten.*"; artikel 71, §1, van de WOG.
[9] Eventuele specifieke regels betreffende de uitoefening van bepaalde politieopdrachten (bv. voor de Directie van de Speciale Eenheden) worden niet in aanmerking genomen voor dit advies.

wettelijkheid, de noodzaak en de evenredigheid van de verwerking van een bijzondere categorie van gegevens, i.e. de vingerafdrukken die biometrische gegevens zijn.

12. De verwerking van dergelijke gegevens in het kader van een intern beleid voor het beheer van de toegang tot andere uitrustingen of lokalen, zoals lokalen bestemd voor in beslag genomen wapens of een ander type materieel zoals radio's, is uitgesloten van het huidige advies.
Dit advies spreekt zich dus niet uit over de verwerking van persoonsgegevens met het oog op het beheer van de toegang tot de politiegebouwen. Het Controleorgaan heeft onlangs een advies uitgebracht over een ontwerp van Koninklijk besluit betreffende de beveiliging van de politiegebouwen en complexen van politiegebouwen[10].

13. Het Controleorgaan vestigt de aandacht op het feit dat de analyse, de ontwikkelingen en de beschouwingen in het advies uit eigen beweging focussen op de aspecten van gegevensbescherming in verband met het beheer van de toegang tot bewapening en worden geformuleerd onverminderd de toepassing van andere wetgeving.

14. De functionele analyse van het beheer van de bewapening moet rekening houden met de organisatorische, strategische en operationele doelstellingen van de politie-entiteit[11] en moet verschillende risicoanalyses en perspectieven integreren zoals, zonder volledigheid na te streven, het welzijn op het werk, de interne organisatie en logistiek (bv. beheer van het materieel, beheer van de werkroosters, …), de veiligheid van de persoonsgegevens[12] en van de informatie enzovoort.
Concreet vereist de bewapening als activa (materieel) van de organisatie de invoering van een beleid van beheer dat het resultaat is van het samenvallen van wettelijke verplichtingen, meer bepaald op het vlak van interne werking en organisatie, bewapening, risicobeheersing en gegevensbescherming.

15. Wat betreft dit punt schaart het COC zich achter de holistische benadering die de AIG aanmoedigt in haar recente rapport waarin ze de balans opmaakt van de laatste jaren van inspecties betreffende de bewapening van de geïntegreerde politie[13], die – hoewel voornamelijk gericht op de controle van de

[10] Een adviesaanvraag inzake een Koninklijk besluit "*betreffende de beveiliging van de politiegebouwen en complexen van politiegebouwen* "werd op 3 april 2023 ingediend bij het Controleorgaan (referentie DA230015). In zijn advies DA230015 spreekt het Controleorgaan zich uit over de eisen van een wettelijke basis voor de verwerking van vingerafdrukken. Dit aspect wordt in het huidige advies verder uitgewerkt.
[11] Meer bepaald: de wet van 7 december 1998 "*tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus*", de wet van 5 augustus 1992 "*op het politieambt*", de normen inzake informatiebeveiliging, de wet van 4 augustus 1996 "*betreffende het welzijn van de werknemers bij de uitvoering van hun werk*" en de Codex over het welzijn op het werk, de omzendbrief CP3 van 29 maart 2011 "*betreffende organisatiebeheersing in de geïntegreerde politie, gestructureerd op twee niveaus*", het Nationaal Veiligheidsplan, de opdrachtbrieven bedoeld in artikel 72 van de wet van 26 april 2002 "*houdende de essentiële elementen van het statuut van de personeelsleden van de politiediensten en houdende diverse andere bepalingen met betrekking tot de politiediensten* "enz..
[12] Artikel 32 van de AVG.
[13] Algemene Inspectie van de federale politie en van de lokale politie, *Omzendbrief GPI 62* "*betreffende de bewapening van de geïntegreerde politie – Balans van de laatste jaren van inspecties*", juli 2022, p. 29, gepubliceerd op www.aigpol.be, geraadpleegd op 6 november 2023.

toepassing van de rondzendbrief GPI 62[14] – aanmoedigt om een methodische en systemische benadering te ontwikkelen om te komen tot een optimaal veiligheidsniveau, rekening gehouden met de correlatie tussen meerdere risico's, inzonderheid die in verband met de veiligheid van de gebouwen en die in verband met de opslag en de bewaking van de bewapening.

16. Het beheer van de risico's in verband met bewapening moet dynamisch zijn en evolueren, waarmee wordt bedoeld dat dit beheer moet worden aangepast in functie van de verworven ervaring, de evolutie van de werkmethoden of de arbeidsvoorwaarden alsook van de technologische middelen.
Het zal onder andere worden geconcretiseerd door de samenvoeging van passende maatregelen zoals, zonder volledigheid na te streven, passende infrastructuur, opleidingen evenals de verwerking van persoonsgegevens met inachtneming van de beginselen van noodzakelijkheid en evenredigheid.

VERWERKING VAN PERSOONSGEGEVENS MET HET OOG OP HET BEHEER VAN DE TOEGANG TOT BEWAPENING

RECHTSKADER – WETTELIJKHEID VAN DE VERWERKING[15]

17. Het Controleorgaan stelde in de informatieverzoeken die het heeft ontvangen vast dat de redenen die voornamelijk worden aangevoerd om het gebruik van vingerafdrukken in het kader van het beheer van de toegang tot bewapening te rechtvaardigen, de veiligheid (van de personeelsleden en van anderen) alsook het toezicht op de naleving van de arbeidsvoorwaarden zijn.
Algemeen is het COC van mening dat het gebruik van de omschrijving "*voor veiligheidsdoeleinden*" te vaag is om een doel van verwerking te definiëren, zeker wanneer de betrokken verwerking van gegevens betrekking heeft op bijzondere gegevens (gevoelige gegevens)[16].

18. Het koninklijk besluit van 3 juni 2007 betreffende de bewapening van de geïntegreerde politie, gestructureerd op twee niveaus[17] ("besluit Bewapening") en de omzendbrief GPI 62, die uitvoering geven aan en toelichting geven bij artikel 141 van de wet van 7 december 1998 "*tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus*" (WGP), stellen verplichtingen en

[14] Omzendbrief GPI 62 van 14 februari 2008 betreffende de bewapening van de geïntegreerde politie, gestructureerd op twee niveaus, zoals gewijzigd op 19 oktober 2017. Zie infra.
[15] Artikel 6 van de AVG.
[16] Controleorgaan op de politionele informatie, Advies uit eigen beweging "*met betrekking tot het invoeren van camerabewaking door de geïntegreerde politie met het oog op de controle van de naleving van de arbeidsvoorwaarden*", BD200007, 17 augustus 2020; Controleorgaan op de politionele informatie, Advies uit eigen beweging "*naar aanleiding van de bevindingen in het kader van een onderzoek naar het gebruik van bodycams*", CON190008, 8 mei 2020.
[17] Koninklijk besluit van 3 juni 2007 "*betreffende de bewapening van de geïntegreerde politie, gestructureerd op twee niveaus, alsook de bewapening van de leden van de Diensten Enquêtes bij de Vaste Comités P en I en van het personeel van de Algemene inspectie van de federale politie en van de lokale politie*".

verantwoordelijkheden vast met betrekking tot bewapening, het bijhouden, dragen, vervoer, opslaan en bewaken van bewapening.

19. Het beheer en de dotatie van bewapening vertegenwoordigen bijgevolg een bijzonder aspect van de verplichtingen inzake interne organisatie, werking en beheer die respectievelijk rusten op de commissaris-generaal, de directeurs-generaal, de administratieve en gerechtelijke directeurs-coördinatoren evenals de korpschefs ten aanzien van hun directie of korps van de lokale politie[18].

20. De bewapening moet inderdaad worden bewaard op een beveiligde plaats, buiten het bereik van derden, overeenkomstig de instructies, naargelang het geval, van de korpschef, de commissaris-generaal, de directeur-generaal, de directeur of de dienstchef[19]. Wanneer de bewapening niet voor een opdracht wordt meegenomen, moet ze worden opgeslagen op een veilige plaats in een infrastructuur van de plaats van tewerkstelling[20].

21. De omzendbrief GPI 62 betreffende de bewapening van de geïntegreerde politie bepaalt met name het volgende: "*De werkgever moet de geschikte maatregelen nemen zodat enkel de personeelsleden die de adequate richtlijnen hebben gekregen in contact kunnen komen met de bewapening en deze kunnen hanteren en om diefstal, verlies of beschadiging te vermijden*"[21] en ook dat "*de genomen maatregelen moeten toelaten dat de toegang tot de bewapening wordt beperkt tot alleen het bevoegde personeel en dat misbruik door onbevoegd personeel niet mogelijk is*"[22].

22. In dit kader kan een intern beleid voor beheer van de toegang tot bewapening de verwerking van persoonsgegevens omvatten met als doel dat alleen de bevoegde personeelsleden in contact kunnen komen met de bewapening en deze kunnen manipuleren.

23. Deze hiervoor vermelde verwerking vormt geen verwerking in de zin van artikel 27 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (WVG). Met andere woorden, in dit geval is er geen sprake van doeleinden van bestuurlijke en gerechtelijke politie en zijn de artikelen 44/1 en volgende van de WPA niet van toepassing.

24. Een dergelijke verwerking vormt een verwerking van persoonsgegevens die behoort tot het toepassingsgebied van de AVG[23].

[18] Artikelen 44 en 98 WGP.
[19] Artikel 19 van het besluit Bewapening.
[20] Artikel 20 van het besluit Bewapening.
[21] Omzendbrief GPI 62, Hoofdstuk I. Dezelfde regels zijn van toepassing in verband met munitie.
[22] Omzendbrief GPI 62, Hoofdstuk VI, Afdeling 2.
[23] Artikel 4, 2) van de AVG.

De verwerking van persoonsgegevens om het beheer van de toegang tot bewapening te verzekeren vertegenwoordigt dus een wettelijke verplichting in de zin van artikel 6.1, c) AVG, die voortvloeit uit de combinatie van wettelijke verplichtingen inzake interne werking en organisatie, bewapening en risicobeheersing. Ze is afkomstig van een gecombineerde lezing van onderstaande bepalingen:

- Wet van 07.12.1998 "*tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus*" (WGP);
    - Artikelen 44, 98 en 141 betreffende het interne beheer en de interne werking alsook betreffende de uitrusting;
- Koninklijk besluit van 03.06.2007 "*betreffende de bewapening van de geïntegreerde politie, gestructureerd op twee niveaus, alsook de bewapening van de leden van de Diensten Enquêtes bij de Vaste Comités P en I en van het personeel van de Algemene inspectie van de federale politie en van de lokale politie*" (hierna "besluit Bewapening");
    - Omzendbrief GPI 62 van 14.02.2008 "*betreffende de bewapening van de geïntegreerde politie, gestructureerd op twee niveaus*";

25. De verwerking van persoonsgegevens van leden van de politiediensten om het beheer van de toegang tot bewapening te verzekeren steunt bijgevolg op een wettelijke verplichting.
De toestemming[24] van de betrokkene (*in casu* het personeelslid van de politie-eenheid) kan dus niet worden ingeroepen als basis voor de wettelijkheid van de verwerking.
Zoals het Controleorgaan al in meerdere van zijn adviezen heeft uiteengezet[25], valt dit te verklaren door het gebrek aan evenwicht (de hiërarchische relatie) tussen het personeelslid (betrokkene) en de overheidsinstantie die beslist om de verwerking uit te voeren (verwerkingsverantwoordelijke)[26].

VERPLICHTINGEN VAN DE VERWERKINGSVERANTWOORDELIJKE

26. De verwerking van persoonsgegevens voor doeleinden van beheer van de toegang tot bewapening behoort dus tot het toepassingsgebied van de AVG. Bijgevolg zijn de beginselen en verplichtingen van de AVG ook van toepassing op deze verwerking. In verband hiermee wordt verwezen naar de relevante artikelen van de AVG[27].
In dit hoofdstuk wordt meer bepaald de nadruk gelegd op sommige van deze aspecten.

[24] Artikel 6.1, a) van de AVG.
[25] Controleorgaan op de politionele informatie, *Advies uit eigen beweging betreffende het filmen door burgers van politie-interventies en betreffende de bescherming van de persoonsgegevens en de privacy van politieambtenaren tegenover derden tijdens de uitvoering van hun politionele opdrachten*, DD200025, 22 november 2021; Controleorgaan op de politionele informatie, *Advies uit eigen beweging met betrekking tot het invoeren van camerabewaking door de geïntegreerde politie met het oog op de controle van de naleving van de arbeidsvoorwaarden*, BD200007, 17 augustus 2020; Controleorgaan op de politionele informatie, *Advies uit eigen beweging naar aanleiding van de bevindingen in het kader van een onderzoek naar het gebruik van bodycams*, CON190008, 8 mei 2020; Controleorgaan op de politionele informatie, *Advies betreffende een aanvraag tot gebruik van een badgesysteem door de politiezone xxx*, DD200013, 1 april 2020, te vinden op www.controleorgaan.be.
[26] Artikel 4.11 en consideransen 32, 42 en 43 van de AVG.
[27] Aangevuld door titel 1 van de WVG en artikel 145 van de WGP.

27. Algemeen is het de taak van de verwerkingsverantwoordelijke om zich te vergewissen van de conformiteit van de verwerking en de veiligheid van de verwerkte persoonsgegevens vóór de verwerking, op het ogenblik van de verwerking en tijdens de uitvoering ervan[28]. De maatregelen die worden genomen om het hoofd te bieden aan de geïdentificeerde risico's, moeten worden geactualiseerd voor de volledige duur van de verwerking en op basis van een dynamisch en continu risicobeheersingsproces.

De documentatie van alle fasen van de bepaling van de verwerking (advies van de DPO, risicoanalyses, …) is belangrijk en maakt het voor de verwerkingsverantwoordelijke mogelijk de conformiteit van de verwerking aan te tonen op eender welk ogenblik en dus ook op verzoek van de toezichthoudende autoriteit.

BESCHERMING VAN DE GEGEVENS VANAF HET ONTWERP (*PRIVACY BY DESIGN*)

28. Krachtens het toepasselijk rechtskader mag de verwerkingsverantwoordelijke gegevens verwerken voor het beheer van de toegang tot bewapening maar moet hij de nadere regels van deze verwerking vaststellen.

In het licht van de toepassing van het beginsel van bescherming van de persoonsgegevens vanaf het ontwerp (*privacy by design*) moet de verwerkingsverantwoordelijke vanaf de vaststelling van de nadere regels van de verwerking toezien op de beoordeling van de noodzaak en van de evenredigheid[29] van de verwerking van de gegevens ten aanzien van het beoogde doel.

Bij wijze van voorbeeld en zonder volledigheid na te streven:

- Welke gegevens zijn noodzakelijk om het doel te bereiken?
- Welke zijn de noodzakelijke verwerkingsverrichtingen (inzamelen, bewaren, wissen enzovoort)?
- Wordt er gebruik gemaakt van een individuele wapenkoffer?
- Moeten er gegevens worden verwerkt om toegang te hebben tot een individuele wapenkoffer?
- Hoe is de individuele wapenkoffer toegankelijk? Met een badge? Een code? Een sleutel? …
- Is er nood aan een slimme kast voor beheer van het middel dat toegang verleent (badge / sleutel / …) tot de individuele wapenkoffer?
- Hoe krijgt men toegang tot het bewapeningslokaal?
- Is er nood aan een slimme kast voor beheer van het middel dat toegang verleent tot het bewapeningslokaal (badge / sleutel / …)?
- Vereist het verlenen van toegang een identificatie of een authenticatie van het personeelslid?
- Hoe lang zouden de gegevens moeten worden bewaard[30]?
- Worden de toegangen geregistreerd in een logboek? Indien ja, welke gegevens worden dan geregistreerd?

[28] Artikelen 5, 24 en volgende van de AVG.
[29] Artikel 5.1, b) en c) van de AVG (principes van minimale gegevensverwerking en doelbinding).
[30] Artikel 5.1, e) van de AVG.

- Hoe lang moeten deze geregistreerde gegevens worden bewaard?
- Wie heeft toegang tot de geregistreerde gegevens en met welke doeleinden?
- Moeten, met uitzondering van de personeelsleden die toegang moeten hebben tot de bewapening met het oog op de uitoefening van hun opdrachten, andere (categorieën van) personen toegang kunnen krijgen tot het lokaal en/of de wapens (onderhoudspersoneel, wapenmaker, brandpreventie,…)? Indien ja, tegen welke voorwaarden?
- …

29. In dit verband moeten de sleutelpersonen die rechtstreeks of onrechtstreeks in verband staan met de uitvoering van de verwerking tijdig worden betrokken bij de denkoefening van de verwerkingsverantwoordelijke; het gaat bijvoorbeeld om de Functionaris voor Gegevensbescherming (DPO) voor voorafgaand en geïnformeerd advies[31], een vertegenwoordiger van de personeelsleden die toegang hebben tot de bewapening voor de uitoefening van hun opdrachten, het personeelslid dat bevoegd is inzake welzijn op het werk, een personeelslid dat belast is met de IT-infrastructuur enzovoort.

30. Terwijl de verwerking van persoonsgegevens een maatregel vormt – naast andere maatregelen – die toelaat het hoofd te bieden aan het geïdentificeerde risico dat inherent is aan de bewapening als activa (materieel) van de organisatie, moet de verwerkingsverantwoordelijke aan de hand van de evaluatie van de noodzaak en de evenredigheid van de verwerking (principes van minimale gegevensverwerking en van doelbinding) aantonen dat hetzelfde resultaat niet op een andere wijze zou kunnen worden bereikt, i.e. met minder indringende middelen op het vlak van gegevensbescherming, bijvoorbeeld de verwerking van andere (categorieën van) gegevens of van minder gegevens[32].

EFFECT- EN RISICOBEOORDELING (GBEB) EN BEVEILIGING VAN DE GEGEVENS[33]

31. Naast de in de vorige punten genoemde risicoanalyses is een effect- en risicobeoordeling van de beoogde verwerking ten aanzien van de bescherming van de persoonsgegevens (hierna "GEB" / *DPIA*[34]) een verplichte voorafgaande voorwaarde wanneer de beoogde verwerking aanleiding kan geven tot een hoog risico voor de rechten en vrijheden van de natuurlijke personen[35], bijvoorbeeld wanneer het gaat om biometrische gegevens.

[31] Artikelen 38 en 39 van de AVG.
[32] Voor zover dienstig, zie meer bepaald de rechtspraak EHRM, BĂRBULESCU t. ROEMENIË, Verzoek nr. 61496/08, 5 september 2017 en EHRM, López Ribalda e.a. t. Spanje, Verzoeken nr. 1874/13 en 8567/13, 17 oktober 2019, betreffende de criteria waaraan maatregelen ten aanzien van de werknemers op hun werkplek moeten voldoen om geen inbreuk te maken op artikel 8.
[33] Artikel 32 van de AVG.
[34] *Data Protection Impact Assessment.*
[35] Artikel 35, §1, van de AVG.

32. De GEB moet *a minima*[36] een stelselmatige beschrijving bevatten van de beoogde verwerkingsverrichtingen en de doeleinden van de verwerking, een evaluatie van de noodzaak en de evenredigheid van de verwerkingsverrichtingen ten aanzien van de doeleinden, een beoordeling van de risico's voor de rechten en vrijheden van de betrokkenen, en de beoogde maatregelen om het hoofd te bieden aan de risico's, met inbegrip van de garanties, maatregelen en veiligheidsmechanismen om de bescherming van de persoonsgegevens te verzekeren en aan te tonen dat de AVG in acht is genomen, rekening gehouden met de rechten en de gerechtvaardigde belangen van de betrokkenen en de andere getroffen personen.

33. Het is de GEB die de verwerkingsverantwoordelijke stuurt[37] bij het bepalen van de passende modaliteiten van de verwerking en die hem dus zal toelaten te verifiëren of de te verwerken gegevens toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden (principe van minimale gegevensverwerking)[38].

34. In verband hiermee wijst het COC erop dat het advies van de Functionaris voor Gegevensbescherming (DPO) moet worden gevraagd in het kader van de uitvoering van de GEB[39].

35. De maatregelen[40] die voortvloeien uit de GEB voor de rechten en vrijheden van de betrokkenen, moeten meer bepaald toelaten antwoord te geven op de volgende aandachtspunten (zonder volledigheid na te streven):

- De ongeoorloofde of onwettige verwerking van de gegevens.
- Het verlies, de vernietiging of de beschadiging van accidentele oorsprong van de gegevens.
- De uitvoering van controleactiviteiten.
  Bijvoorbeeld: de controle van de toegang tot de bewapening; de toegang tot de registratie van de toegang tot bewapening; voorwaarden en doeleinden van de toegang tot de registratie van de toegang tot bewapening.
- De intrekking van de rechten.
  Bijvoorbeeld: de intrekking van het recht van toegang tot bewapening; de controle van de conformiteit van de verleende toegangsrechten.
- Vertrouwelijkheid van de gegevens.

---

[36] Artikel 35, §7, van de AVG.
[37] Voor zover dienstig, zie de Beslissing betreffende de aanname van de lijst met verwerkingen waarvoor een Gegevensbeschermingseffectbeoordeling dient te worden uitgevoerd conform artikel 35.4 van de Algemene Verordening Gegevensbescherming, 01/2019 van 16 januari 2019, te raadplegen op https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-nr.-01-2019-van-16-januari-2019.pdf, geraadpleegd op 6 november 2023.
Aanbeveling uit eigen "*beweging met betrekking tot de gegevensbeschermingseffectbeoordeling en voorafgaande raadpleging*", 01/2018 van 28 februari 2018, te raadplegen op https://www.gegevensbeschermingsautoriteit.be/publications/aanbeveling-nr.-01-2018.pdf, geraadpleegd op 6 november 2023.
[38] Artikel 5, §1, c) van de AVG.
[39] Artikel 35, §2, van de AVG en artikel 22 van de WVG.
[40] Artikel 5.1, f) van de AVG.

Bijvoorbeeld: methode van cryptografie; noodzaak van pseudonimisering van de gegevens; noodzaak van bewaring van het niet getransformeerd of ongecodeerd gegeven (bv. indien het gegeven wordt omgezet in een code).

- Traceerbaarheid / registratie.
  Bijvoorbeeld: geregistreerde persoonsgegevens en informatie; bewaartermijn van de geregistreerde persoonsgegevens.
- Beheer van de inbreuken op gegevens.
  Bijvoorbeeld: verdeling van de rollen en verantwoordelijkheden in geval van inbreuk op gegevens of inbreuk op de beveiliging; vaststellen en communiceren van een interne procedure.

JUISTHEID EN ACTUALISERING VAN DE GEGEVENS[41]

36. Het is de taak van de verwerkingsverantwoordelijke om de noodzakelijke en passende technische en organisatorische maatregelen te nemen om zich te vergewissen van het feit dat de gegevens die toegang mogelijk maken, enkel betrekking hebben op de gemachtigde personeelsleden, i.e. zij die voldoen aan de toegangsvoorwaarden (opleiding, effectief lid van de eenheid, machtiging, doel, …).

Dit impliceert inzonderheid dat de diensten die al dan niet rechtstreeks betrokken zijn bij de uitvoering van de verwerking worden geïntegreerd en tijdig communiceren met de verantwoordelijke voor het toegangsbeheer (hiërarchische verantwoordelijken, dienst voor intern toezicht, …).
Bijvoorbeeld: de gegevens van een personeelslid van wie de toegang tot de bewapening moet worden ingetrokken wegens een verandering van eenheid of een lopend (gerechtelijk / tuchtrechtelijk) onderzoek moeten onmiddellijk kunnen worden bijgewerkt (tijdelijk toegangsverbod, wissen van de gegevens, interne richtlijnen betreffende de communicatie aan de verantwoordelijke voor het toegangsbeheer enzovoort).

37. Nog steeds bij wijze van voorbeeld zou de toegang tot de bewapening afhankelijk kunnen worden gesteld van meerdere voorwaarden waaraan moet zijn voldaan:

- geregistreerd zijn als personeelslid van de eenheid in de applicatie voor personeelsbeheer;
- in orde zijn wat betreft verplichte opleidingen voor wapenbezit;
- toegang tijdens de diensturen;
- enzovoort.

38. Zowel technische maatregelen (bv. waarschuwingssysteem) als organisatorische maatregelen (bv. verificatie *a posteriori* door de bevoegde hiërarchische meerdere) zouden echter moeten toelaten te

[41] Artikel 5.1, d) van de AVG.

anticiperen op uitzonderlijke situaties zoals het feit dat het wapen niet wordt teruggegeven na afloop van de dienst of de noodzaak om toegang te hebben tot de bewapening buiten de diensturen (bv. indien een personeelslid zijn dienst moet hervatten buiten de diensturen).

VERWERKING

39. In het geval waarin de verwerkingsverantwoordelijke een beroep wenst te doen op een externe partner om de verwerking uit te voeren, moet hij zich er op voorhand van vergewissen dat de externe partner, een verwerker in de zin van de AVG[42], voldoende garanties biedt inzake de toepassing van passende technische, organisatorische en veiligheidsmaatregelen opdat de rechten van de personeelsleden zouden worden geëerbiedigd[43]. Het kader waarin de verwerker de verwerking verricht, moet nauwkeurig worden vastgesteld in samenspraak met de verwerkingsverantwoordelijke. Zonder volledigheid na te streven moeten de volgende vragen een antwoord krijgen:

- Welke zijn de (categorieën van) gegevens en de categorieën van betrokkenen die de verwerker verwerkt voor rekening van de verwerkingsverantwoordelijke?
- Tot welke gegevens heeft de verwerker toegang?
- Volgens welke modaliteiten heeft de verwerker toegang tot de gegevens?
- Heeft de verwerker een Functionaris voor Gegevensbescherming aangewezen?
- Welke zijn de verplichtingen van de verwerker?
  Bijvoorbeeld: detectie van veiligheidsincidenten; communicatie in geval van veiligheidsincident; samenwerking in geval van uitoefening van de rechten door de betrokkene; …
- Enzovoort.

BEVORDERING VAN DE UITOEFENING VAN RECHTEN DOOR BETROKKENEN[44]

40. De informatie betreffende de rechten van de betrokkenen (personeelsleden) moet worden geformuleerd op kwaliteitsvolle en verstaanbare wijze, bijvoorbeeld in een reglement, een dienstorder of nog bij de verspreiding van de interne richtlijnen die toepasselijk zijn inzake bewapening[45]; de informatie moet ook begrijpelijk en toegankelijk zijn voor de betrokkenen, i.e. personeelsleden die toegang tot bewapening genieten volgens de toepasselijke voorwaarden[46].

[42] Artikel 4.8 van de AVG.
[43] Meer bepaald de artikelen 25, 28 en 29 van de AVG en de artikelen 21 en 22 van de WVG.
[44] Artikelen 12 en volgende van de AVG.
[45] Omzendbrief GPI 62.
[46] Considerans 50 AVG. Zie in dit verband de uiteenzetting van het Controleorgaan in zijn advies uit eigen beweging BD200007 "*met betrekking tot het invoeren van camerabewaking door de geïntegreerde politie met het oog op de controle van de naleving van de arbeidsvoorwaarden*" van 17 augustus 2020, te vinden op www.controleorgaan.be ; Controleorgaan op de politionele informatie, Advies DD200013 "*betreffende een aanvraag tot gebruik van een badgesysteem door de politiezone X*", 1 april 2020, te vinden op www.controleorgaan.be.

De uitoefening van de rechten van de betrokkene doet echter geen afbreuk aan andermans rechten[47].

41. Het Controleorgaan is van mening dat de registratie van de toegang tot bewapening kan worden gebruikt voor tuchtrechtelijke doeleinden. Hetzelfde geldt in het geval waarin er een vermoeden bestaat of het bewijs is geleverd van een strafrechtelijke overtreding[48]. Het betreft de verwerking voor een ander en later doel, dat toelaatbaar is onder bepaalde voorwaarden die het Controleorgaan al heeft genoemd in andere adviezen[49].

VERWERKING VAN VINGERAFDRUKKEN MET HET OOG OP HET BEHEER VAN DE TOEGANG TOT BEWAPENING

42. We herinneren eraan dat titel 2 van de WVG en artikel 44/1 §2, van de WPA in dit geval niet van toepassing zijn daar het gaat om een verwerking die niet de doelstellingen van artikel 27 van de WVG nastreeft en onder het toepassingsgebied valt van de AVG, aangevuld door titel 1 van de WVG.

43. Artikel 9 van de AVG omgeeft de biometrische gegevens – die worden beschouwd als een bijzondere categorie van persoonsgegevens – met specifieke waarborgen. De AVG definieert biometrische gegevens als "*persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijke persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukgegevens*"[50].

44. De verwerking van vingerafdrukken met als doel dat alleen de gemachtigde personeelsleden in contact kunnen komen met bewapening en die kunnen hanteren (toegangsbeheer) vormt dus een verwerking van biometrische gegevens in de zin van artikel 9 van de AVG.
De omzetting van deze vingerafdrukken in een code leidt niet tot een andere conclusie daar deze code de digitale vertaling en de materialisatie is van de vingerafdrukken van het personeelslid. Daar het personeelslid kan worden geïdentificeerd aan de hand van deze code en de verwerking als doel heeft hem op unieke en zekere wijze te identificeren (authenticatie), zijn zowel de vingerafdrukken als de code die deze persoonsgegevens omzet te beschouwen als biometrische gegevens[51].

---

[47] Artikel 15.4 van de AVG. Voor zover dienstig, zie de beslissing van de Geschillenkamer van de Gegevensbeschermingsautoriteit van 29 juli 2020, *Klacht van x tegen y (Recht van toegang bij de gewezen werkgever)*, 41/2020, paragraaf 39 en HJEU, *arrest Peter Nowak t. Data Protection Commissioner*, C-434/16, 20 december 2017.
[48] Zie meer bepaald Hof van Justitie van de Europese Unie, Digi Távközlési és Szolgáltató Kft. t. Nemzeti Adatvédelmi és Információszabadság Hatóság, 20 oktober 2022, C-77/21, §§ 25 e.v.
[49] Bijvoorbeeld voornoemd advies BD200007 van het Controleorgaan op de politionele informatie. Zie specifiek artikel 6.4 AVG.
[50] Artikel 4, 14) van de AVG.
[51] Verslag van het Controleorgaan op de politionele informatie (COC) "*betreffende de visitatie bij een politiezone in de provincie West-Vlaanderen door het Controleorgaan op de politionele informatie in het kader van zijn controle- en toezichtsbevoegdheden*", CON20008, 12 januari 2021, publieke versie te vinden op www.controleorgaan.be.

45. Onderstaande elementen zijn strikt beperkt tot de kwestie van de verwerking van de vingerafdrukken en/of de code die ze omzet voor doeleinden van beheer van de toegang tot bewapening.

De verwerking van andere soorten biometrische gegevens (bv. gezichtsherkenning, herkenning via de iris in het oog, …) is uitgesloten van het huidige advies en dat geldt ook voor de verwerking van biometrische gegevens (in het algemeen) voor het beheer van de toegang tot andere zones van een politiegebouw of tot een politiegebouw[52].

46. Paragraaf 1 van artikel 9 van de AVG voert een verbod in op het beginsel van verwerking van vingerafdrukken.
Paragraaf 2 van hetzelfde artikel bevat een volledige lijst van uitzonderlijke omstandigheden waarin deze gegevens echter mogen worden verwerkt. Artikel 9 van de WVG stelt bijkomende voorwaarden vast waaraan moet worden voldaan voor de verwerking van dergelijke gegevens.

47. Zoals hierboven gezegd, vindt de verwerking van persoonsgegevens met het oog op het beheer van de toegang tot bewapening een wettelijke basis in de gecombineerde lezing van artikel 6.1, c) van de AVG en de artikelen 44, 98 en 141 WGP alsook in het "besluit Bewapening".
De verwerking van bijzondere gegevens – *in casu* de vingerafdrukken – voor hetzelfde doel moet **bovendien** een grondslag vinden onder de uitzonderlijke omstandigheden zoals bedoeld in artikel 9, §2, van de AVG.
Met het oog op het beheer van de toegang tot bewapening en op basis van de voorwaarden zoals bedoeld in artikel 9, §2, van de AVG, is er reden om drie hypothesen te onderzoeken, namelijk:

1) De toestemming (artikel 9, §2, a) AVG);
2) De uitvoering van verplichtingen of de uitoefening van rechten inzake recht op arbeid, sociale zekerheid en sociale bescherming (artikel 9, §2, b) AVG);
3) Om redenen van zwaarwegend algemeen belang op basis van het recht van de Unie of het recht van een lidstaat die bovendien evenredig moet zijn met het beoogde doel (artikel 9, §2, g) AVG).

DE TOESTEMMING (ARTIKEL 9, §2, A) AVG)

48. Zoals hierboven gezegd in het huidige advies kan de **toestemming** van het personeelslid van de politie-entiteit geen wettelijke grondslag vormen voor de betreffende verwerking wegens het ontbreken van de "vrije" aard van deze toestemming, daar het personeelslid zich in een strikt hiërarchische relatie bevindt ten overstaan van de verwerkingsverantwoordelijke.

[52] Zie voornoemd advies DA230015 van het Controleorgaan.

De toestemming zal immers geen afdoende juridische grondslag vormen voor de verwerking in dit geval om er een onevenwicht tussen de betrokkene en de verwerkingsverantwoordelijke, meer bepaald wanneer de verwerkingsverantwoordelijke een overheidsinstantie is – hier de politie-entiteit – en het onwaarschijnlijk is dat de toestemming vrij is gegeven, gelet op de omstandigheden van deze bijzondere situatie[53].

49. In het geval waarin de toestemming toelaatbaar zou zijn – *quod non*, moet de verwerking van de vingerafdrukken strikt noodzakelijk zijn. Het feit dat een alternatief voor de verwerking van de vingerafdrukken wordt *voorgesteld*, zoals het gebruik van een badge of een persoonlijke pincode, voldoet niet aan deze voorwaarde.
Bovendien bewijst het feit dat een dergelijk alternatief voor de verwerking van de vingerafdrukken aan het personeelslid kan worden voorgesteld dat er niet is voldaan aan het beginsel van minimale gegevensverwerking (evenredigheid) van de gegevens[54]: door dit voorstel te doen aan de betrokkene, toont de verwerkingsverantwoordelijke zelf aan dat de verwerking van andere gegevens – die geen bijzondere gegevens zijn in de zin van artikel 9 AVG – het mogelijk maakt hetzelfde doel te bereiken.

UITVOERING VAN VERPLICHTINGEN OF UITOEFENING VAN RECHTEN INZAKE RECHT OP ARBEID, SOCIALE ZEKERHEID EN SOCIALE BESCHERMING (ARTIKEL 9, §2, B) AVG)

50. Artikel 9, §2, b) AVG verwijst naar **de uitvoering van de verplichtingen en de uitoefening van de rechten van de verwerkingsverantwoordelijke of van de betrokkene** inzake het recht op arbeid, sociale zekerheid en sociale bescherming, voor zover deze verwerking wordt toegestaan door het Unierecht, het recht van een lidstaat of door een collectieve overeenkomst die is gesloten krachtens het recht van een lidstaat en die voorziet in passende garanties voor de fundamentele rechten en de belangen van de betrokkene. Op het ogenblik van redactie van het huidige advies bestaat er in België geen dergelijke bepaling van intern recht of dergelijke wettelijke basis.

51. De opmaak van een collectieve arbeidsovereenkomst of een gelijkwaardig document zou hoe dan ook niet volstaan in het huidige geval, aangezien er daarvoor een wettelijke grondslag zou moeten worden gevonden in een (formele) wet.
In dit geval zou er reden zijn om te voorzien in passende garanties voor de fundamentele rechten en belangen van de betrokkenen (personeelsleden), maar dit is enkel van toepassing wanneer blijkt dat vingerafdrukken in deze context mogen worden verwerkt, *quod non*,daar een dergelijk document het ontbreken van een (formele) wettelijke grondslag voor de verwerking niet kan verhelpen.

[53] Considerans 43 van de AVG. Voor zover dienstig, zie *European Data Protection Board*, Richtsnoeren 5/2020 over de toestemming in de zin van Verordening (EU) 2016/679, 4 mei 2020.
[54] Zie infra.

REDEN VAN ZWAARWEGEND ALGEMEEN BELANG (ARTIKEL 9, §2, G) AVG)

52. Artikel 9, §2, g) AVG verwijst dan weer naar de **reden van zwaarwegend algemeen belang** op basis van het Unierecht of van het recht van een lidstaat die evenredig moet zijn ten opzichte van het doel, de essentie van het recht op gegevensbescherming in acht moet nemen en ook moet voorzien in passende en specifieke maatregelen voor de bescherming van de fundamentele rechten en de belangen van de betrokkene.
Op het ogenblik van redactie van het huidige advies uit eigen beweging bestaat er in België geen dergelijke bepaling van intern recht of dergelijke wettelijke basis.
Zo heeft het Controleorgaan er onlangs in zijn advies DA230015 nog op gewezen dat er "*in de Belgische rechtsorde geen algemene nationale wettelijke basis voorhanden is die de verwerking van biometrische persoonsgegevens omkadert. De potentiële wettelijke basis zal duidelijk moeten stellen welke doeleinden als een 'zwaarwegend algemeen belang' worden beschouwd.*"[55].

53. De aanbeveling van de Gegevensbeschermingsautoriteit (GBA) betreffende de verwerking van biometrische gegevens bevestigt dit in volgende bewoordingen: "*(…) heeft de Belgische wetgever er niet voor geopteerd om te voorzien in een algemene wettelijke grondslag die de verwerking van biometrische gegevens in het raam van de unieke identificatie of authenticatie van een persoon voor beveiligingsdoeleinden toelaat. Het ontbreken van een dergelijke wettelijke grondslag brengt met zich mee dat de verwerking van biometrische gegevens, op heden, en met uitzondering van de verwerking van de biometrische gegevens in het kader van de eID (elektronische identiteitskaart) (en het paspoort), niet rechtsgeldig gesteund kan worden op redenen van zwaarwegend algemeen belang.*"[56].
Diezelfde GBA besluit: "*Dit betekent concreet dat de Belgische wetgever de modaliteiten van de verwerking van biometrische gegevens zal moeten neerleggen in de wet in zover zij het gebruik van biometrische gegevens in een bepaalde context wil (blijven) toestaan.*"[57].

54. In het licht van de door de AVG vastgestelde regels en beginselen moet het Controleorgaan dus vaststellen dat de verwerking van de vingerafdrukken van personeelsleden van de geïntegreerde politie met het oog op het beheer van de toegang tot bewapening dat toelaat dat alleen gemachtigde personeelsleden van de geïntegreerde politie toegang krijgen tot bewapening en die mogen hanteren op zijn minst <u>zeer problematisch</u> is wegens het ontbreken van een wettelijke grondslag die de verwerking

[55] Controleorgaan op de politionele informatie, voornoemd advies DA230015, §12.
[56] Zoals hierboven gezegd, is het Controleorgaan van mening dat het gebruik van de omschrijving "*voor veiligheidsdoeleinden*" te vaag is om een doel te definiëren, en dat zeker in het kader van de verwerking van bijzondere gegevens zoals vingerafdrukken.
[57] Gegevensbeschermingsautoriteit, *Aanbeveling betreffende de verwerking van biometrische gegevens*, versie van 1 december 2021, p. 26. Zie concreet het advies van de Gegevensbeschermingsautoriteit van 9 maart 2022 *m.b.t. een voorontwerp van wet tot wijziging van het Belgisch Scheepvaartwetboek betreffende de maritieme beveiliging*, 51/2022, te vinden op www.gegevensbeschermingsautoriteit.be.

van dergelijke bijzondere gegevens expliciet zou toestaan voor een welomschreven doel en die passende garanties zou bieden voor de fundamentele rechten en de belangen van de betrokkenen (personeelsleden van de geïntegreerde politie).

BESCHOUWINGEN

55. Naast de bovenstaande louter juridische beschouwingen merkt het Controleorgaan op dat er op het niveau van de geïntegreerde politie[58] een zekere neiging bestaat om vingerafdrukken van de personeelsleden te verwerken in het kader van een beleid van beheer van de toegang tot bewapening; tevens bestaat er op politiek niveau ernstige bezorgdheid wat betreft de veiligheid van de politionele infrastructuren die inzonderheid heeft geleid tot een omzendbrief evenals een ontwerp van Koninklijk besluit die onlangs voor advies werden overgelegd aan het COC[59].

56. Anticiperend op een eventueel wetgevend initiatief wenst het COC hierna enkele algemene beschouwingen te formuleren betreffende de minimale eisen van de wettelijke grondslag die een expliciet kader zou vormen voor de verwerking van vingerafdrukken van personeelsleden van de geïntegreerde politie met het oog op het beheer van de toegang tot bewapening.

57. Het Controleorgaan is van mening dat het passender zou zijn om de WGP te wijzigen. Het Controleorgaan wijst erop dat elk wetgevend initiatief voor advies aan dit orgaan moet worden overgelegd.
Eerst en vooral is het duidelijk dat, indien de wetgever een algemenere positie zou wensen in te nemen ten aanzien van de verwerking van vingerafdrukken voor toegangsbeheer (niet alleen m.b.t. de politionele bewapening maar bijvoorbeeld ook voor de toegang tot politionele, nucleaire, militaire,… infrastructuur), een volwaardige wet of ten minste een hoofdstuk in de WGP de voorkeur zou wegdragen[60].

58. De rechtspraak[61] heeft meermaals herhaald dat, om een schending van artikel 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM) te vermijden, een inmenging "*wettelijk moet worden*

[58] Dat blijkt meer bepaald uit de verschillende ontvangen informatieverzoeken.
[59] Zie onder andere: Adviesaanvraag "*betreffende het ontwerp van Koninklijk besluit betreffende de beveiliging van de politiegebouwen en complexen van politiegebouwen*", op 3 april 2023 ingediend bij het Controleorgaan (referentie DA230015); Ministeriële omzendbrief GPI 91 van 30 april 2019 over de 'Minimale normen voor beveiliging van het onthaal'; Parlementaire vraag nr. 308 van 4 februari 2021 (Frans) aan de minister van Binnenlandse Zaken, Institutionele Hervormingen en Democratische Vernieuwing, referentie DO 2020202107872 over de maatregelen ter bescherming van de politionele infrastructuur; Parlementaire vraag nr. 632 van 25 mei 2021 (Frans) aan de minister van Binnenlandse Zaken, Institutionele Hervormingen en Democratische Vernieuwing, referentie DO 2020202110214 betreffende de bijkomende maatregelen inzake fysieke bescherming in de omgeving van de commissariaten.
[60] In dit verband wordt verwezen naar de beschouwingen in voornoemd advies DA230015 van het COC.
[61] Meer bepaald: Europees Hof voor de Rechten van de Mens, Nuh Uzun e.a. t. Turkije, verzoek nr. 49341/18, 29 maart 2022; Europees Hof voor de Rechten van de Mens, Rotaru t. Roemenië, verzoek nr. 28341/95, 4 mei 2000; Grondwettelijk Hof, arrest nr. 33/2022 van 10 maart 2022.

vastgesteld', een legitiem doel moet hebben ten aanzien van paragraaf 2 en, bovenal, noodzakelijk moet zijn in een democratische samenleving om dit doel te bereiken. De essentiële elementen van de verwerking moeten worden vastgelegd in de wet zelf (zie artikel 22 van de Grondwet) en dat in duidelijke en voldoende nauwkeurige bewoordingen.

59. Het vereiste niveau van nauwkeurigheid van de betrokken wetgeving – die overigens niet alle mogelijke gevallen kan omschrijven – is natuurlijk afhankelijk van het domein dat ze wordt geacht te bestrijken en van het aantal en de hoedanigheid van de ontvangers[62]: er kan worden overwogen om praktische richtlijnen met beperkte verspreiding aan te nemen. Zo oordeelde het Europees Hof voor de Rechten van de Mens dat de vereiste inzake voorzienbaarheid in domeinen met betrekking tot de nationale veiligheid niet dezelfde draagwijdte kon hebben als in andere domeinen[63].

60. Zoals reeds gesteld met betrekking tot de beveiliging van de politiegebouwen en complexen van politiegebouwen[64], legt het Controleorgaan de nadruk op het feit dat een verwerking zoals die waarvan sprake niet kan worden geregeld bij koninklijk besluit en dat de loutere aanpassing van het Koninklijk besluit Bewapening en/of een omzendbrief zoals de GPI 62 in dit geval onvoldoende zou zijn.
In de hypothese van een wetgevend initiatief zou het al dan niet verplichte karakter van het gebruik van een dergelijke verwerking voor het doel van beheer van de toegang tot bewapening moeten worden geïdentificeerd.

61. Gelet op de bijzonder gevoelige aard van vingerafdrukken zouden de bevoegde ministers een evaluatie moeten maken van de toegevoegde waarde die wordt geboden door de toepassing van een dergelijke verwerking op geïntegreerde wijze, i.e. via de toepassing van uniforme technische, organisatorische en veiligheidsmaatregelen binnen de politie-entiteiten die deze verwerking uitvoeren. Bij wijze van voorbeeld en zonder volledigheid na te streven:

- categorieën van verwerkte biometrische gegevens (vingerafdrukken, …);
- type verwerkte gegevens (onbewerkte vingerafdrukken of hun omzetting in een code (profiel));
- hoogte van de drempel voor validatie van de identificatie[65];
- type vergelijking (eenvoudige identificatie of authenticatie)[66];
- detectie, melding en opvolging van veiligheidsincidenten;
- minimale inhoud van de interne richtlijnen;
- gegevens die moeten worden geregistreerd;
- minimale bewaartermijn van de geregistreerde gegevens;

[62] Europees Hof voor de Rechten van de Mens, Grote Kamer, 4 december 2008, S. en Marper t. Verenigd Koninkrijk.
[63] Europees Hof voor de Rechten van de Mens, 26 maart 1987, Leander t. Zweden; Europees Hof voor de Rechten van de Mens, 4 juli 2006, Lupsa t. Roemenië; Grondwettelijk Hof, arrest nr. 33/2022 van 10 maart 2022.
[64] Controleorgaan op de politionele informatie, voornoemd advies DA230015.
[65] Voor meer informatie, zie Gegevensbeschermingsautoriteit, voornoemde *Aanbeveling betreffende de verwerking van biometrische gegevens*.
[66] *Ibidem*.

- …

62. In dit opzicht zou de betrokkenheid van de diensten die een algemene rol of een ondersteunende rol inzake logistiek[67] ten aanzien van de verwerkingsverantwoordelijke vervullen, moeten worden onderzocht.
De omstandige adviezen van het Coördinatiecomité van de geïntegreerde politie[68] en van het Strategisch adviescomité voor informatie[69] zouden ter zake onbetwistbaar toegevoegde waarde bieden.

63. Hoe dan ook legt het Controleorgaan de nadruk op het feit dat het bestaan van een wettelijke grondslag in de zin van artikel 9, §2, b) of g) van de AVG niet zou volstaan opdat de bewuste verwerking, voor het beoogde doel, conform zou zijn aan de AVG. Naast de wettelijke grondslag moet er immers worden voorzien in passende aangepaste en aanvullende garanties in de zin van artikel 9 van de WVG alsook in de naleving van de algemene beginselen en andere regels van de AVG.

64. In dit verband wenst het COC het inzonderheid de aandacht te vestigen op het evenredigheidsbeginsel: het is de taak van de verwerkingsverantwoordelijke om te verifiëren en voorafgaand aan en voor de hele duur van de verwerking te kunnen aantonen dat die verwerking conform is met alle toepasselijke regels en voorwaarden, met inbegrip van het feit dat de verwerkte gegevens toereikend en ter zake dienend zijn en beperkt tot wat noodzakelijk is ten opzichte van het doel waarvoor de gegevens worden verwerkt (principe van minimale gegevensverwerking)[70].

65. De omzendbrief GPI 62[71] bepaalt dat de wapenlokalen enkel toegankelijk mogen zijn door toepassing van een specifieke procedure die de verantwoordelijke voor het lokaal moet vaststellen zodat alleen een beperkt aantal personen die hij speciaal aanwijst toegang tot dat lokaal kunnen hebben. Er kan bijvoorbeeld toegang worden verleend met behulp van een badge of een toegangscode. Er moet een passende procedure worden uitgewerkt voor inbezitneming en teruggave van de wapens, desgevallend via een gebruikersregister met vermelding van de naam van de gebruiker van het wapen, de datum IN en de datum OUT. Deze procedure moet worden aangepast in functie van de plaatselijke omstandigheden (aantal wapens, personeelssterkte, plaatsconfiguratie, …). Hoe dan ook moet de procedure zodanig worden opgevat dat de toegang tot het opslaglokaal wordt beperkt tot enkel het

[67] Zonder volledigheid na te streven: het Commissariaat-generaal (artikel 100*bis*, §1, WGP), de algemene directie van het middelenbeheer en de informatie (artikel 93, §1, 2°, WGP en artikel 6 van het koninklijk besluit van 14 november 2006 betreffende de organisatie en de bevoegdheden van de federale politie), de coördinatie- en steundirecties (artikel 104 WGP en artikel 4 van het Koninklijk besluit van 14 november 2006 "*betreffende de organisatie en de bevoegdheden van de federale politie*".
[68] Gelet op zijn adviesopdracht zoals bedoeld in artikel 8*ter*, §2 WGP.
[69] Gelet op zijn steunopdracht zoals bedoeld in artikel 8*sexies*, §2 WGP.
[70] Met betrekking tot de vereiste van evenredigheid en ter informatie verwijst de GBA in haar voornoemde aanbeveling van 2021 als voorbeeld naar een vonnis van de rechtbank van Amsterdam die van oordeel was dat het gebruik van een scan van vingerafdrukken die de toegang mogelijk maakte tot het kassysteem in een winkel, om de veiligheid en de integriteit van bijzondere gegevens te verzekeren en elke vorm van fraude te voorkomen, onevenredig was. Zoals benadrukt door de GBA heeft de winkel onvoldoende aangetoond dat er geen minder radicaal alternatief bestond om hetzelfde doel te bereiken. De toegang tot de kassa in een winkel brengt natuurlijk niet dezelfde risico's mee als de toegang van leden van de geïntegreerde politie tot de bewapening om hun opdrachten uit te oefenen.
[71] Omzendbrief GPI 62, Hoofdstuk VI, Deel 2.

gemachtigd personeel, dat de toegang wordt gecontroleerd, dat het aantal opgeslagen wapens gemakkelijk kan worden gecontroleerd, dat onrechtmatig gebruik door onbevoegd personeel onmogelijk is en dat de sleutels desgevallend niet op de deur van het versterkt lokaal blijven steken.

66. Gelet op het feit dat het gebruik van een badge of een toegangscode zoals vermeld in de omzendbrief GPI 62 een suggestie is, moet de beoordeling van de evenredigheid natuurlijk rekening houden met de technologische ontwikkelingen evenals de mogelijkheid van combinatie van meerdere methoden van toegangsbeheer, waarbij steeds de geactualiseerde risicobeoordeling en de uitgevoerde functionele analyse in aanmerking moeten worden genomen[72].

67. Ook de ervaring van de verwerkingsverantwoordelijke of zelfs van andere entiteiten van de GPI (bv. het zich voordoen van een incident) is een aandachtspunt[73]. Een verwerking van persoonsgegevens op basis van voornamelijk (of zelfs uitsluitend) of eerder "emotionele" argumenten en/of een niet gedocumenteerd anticiperen op het als ernstigst beschouwde risico is echter onvoldoende.

In dit opzicht ziet het Controleorgaan bijvoorbeeld niet in welke mate de verwerking van de vingerafdrukken van de personeelsleden bij de ingang van het wapenlokaal als enig middel voor toegangsbeheer evenredig zou zijn, zeker indien de bewapening als zodanig niet is opgeborgen in individuele lockers waarvan de toegang wordt geblokkeerd of in ieder geval wanneer, eens de toegang tot het lokaal geopend is, het personeelslid de mogelijkheid heeft om bezit te nemen van een of meerdere wapens dat (die) niet voor hem is (zijn) bestemd.

68. Hoe dan ook moet de verwerkingsverantwoordelijke aantonen dat de verwerking van de vingerafdrukken onvermijdelijk is ten opzichte van andere maatregelen en de (eventueel gecombineerde) verwerking van andere gegevens zoals de tussenkomst van een wapenmaker, het gebruik van een badge, een pincode, beveiligde individuele lockers, bewakingscamera's, *MFA*-middelen enz. om het beoogde doel te bereiken, rekening gehouden met de belangen, de rechten en de vrijheden van de betrokkenen en de beoogde doeleinden alsook eventuele geïdentificeerde risico's.

69. Evenzo zouden de risicoanalyses en de functionele analyse in verband met de bewapening moeten aantonen dat er een onderscheid moet worden gemaakt tussen de toegang tot het bewapeningslokaal en tot elk wapen: is het de bedoeling dat logistiek personeel toegang kan hebben tot het lokaal voor

[72] In dit verband wordt de verwerking van biometrische gegevens voor doeleinden van authenticatie (te begrijpen als de validatie van de identificatie) erkend als een sterk authenticatiemiddel zoals ook de multifactorauthenticatie (*Multi-Factor Authentification – MFA*) (Commissie voor de bescherming van de persoonlijke levenssfeer, *Advies uit eigen beweging over het verwerken van biometrische gegevens in het raam van authenticatie van personen*, nr. 17/2008, 9 april 2008, p. 10, te vinden op https://www.gegevensbeschermingsautoriteit.be/publications/advies-nr.-17-2008.pdf, geraadpleegd op 6 november 2023).
[73] Ter informatie geven we mee, wat betreft het gebruik van bewakingscamera's met het oog op de controle van de naleving van de arbeidsvoorwaarden, dat de rechtspraak al heeft aangegeven dat er ook niet wordt geëist dat de verwerkingsverantwoordelijke eerst nadeel heeft geleden alvorens camerabewaking te mogen invoeren (Hof van Justitie, 11 december 2019, TK, C-708/18, considerans 44).

bijzondere opdrachten (bv. schoonmaken, een gloeilamp vervangen, …) zonder dat die personen toegang kunnen hebben tot de bewapening omdat ze daartoe niet gemachtigd zijn? Het is duidelijk dat de toegang tot bewapening via de verwerking van vingerafdrukken niet in alle opzichten zal kunnen worden gerechtvaardigd.

CONCLUSIE

70. De verwerking van persoonsgegevens van personeelsleden van een politie-entiteit met het oog op het beheer van de toegang tot bewapening behoort tot het toepassingsgebied van de AVG.
Deze verwerking vindt een wettelijke grondslag in het samenvallen van wettelijke verplichtingen inzake interne werking en organisatie, bewapening en risicobeheersing[74].

71. Vingerafdrukken – en ook de code (profiel) die deze omzet – vormen zogenaamde bijzondere gegevens in de zin dat ze bijzondere garanties en bescherming genieten.
De verwerking van vingerafdrukken van het personeel van de geïntegreerde politie met het oog op het beheer van de toegang tot bewapening moet dus een rechtsgrond krijgen onder de uitzonderlijke voorwaarden bedoeld in artikel 9 §2, AVG.

72. Hoewel het Controleorgaan begrip heeft voor de belangstelling van de geïntegreerde politie voor de verwerking van vingerafdrukken in het kader van een intern beleid van toegangsbeheer opdat alleen gemachtigde personeelsleden in aanraking zouden kunnen komen met bewapening en de hantering ervan, moet het COC vaststellen, in het licht van de regels en principes die de AVG heeft vastgesteld en in de huidige stand van de Belgische wetgeving, dat een dergelijke verwerking **zeer problematisch** is wegens het ontbreken van een wettelijke grondslag die de verwerking van dergelijke bijzondere gegevens voor dit doel uitdrukkelijk zou toelaten en die passende garanties zou bieden voor de fundamentele rechten en de belangen van de betrokkenen[75].

73. Het Controleorgaan wijst erop dat de toestemming van de betrokkene[76] geen rechtsgrond kan vormen voor de verwerking, daar zou kunnen worden beschouwd dat de toestemming niet vrijlijk en met kennis van zaken is gegeven. Het feit dat de verwerkingsverantwoordelijke aan de betrokkene voorstelt om vrij te kiezen tussen de verwerking via vingerafdrukken of, bijvoorbeeld, een code heeft geen impact op het ontbreken van het vrije karakter van de toestemming. Bovendien is het aanbieden van een dergelijk alternatief het bewijs op zich van het ontbreken van de onvermijdelijk karakter van de verwerking van deze gegevenscategorie.

74. Bovendien moet in herinnering worden gebracht dat de wettelijke basis van de verwerking niet stelselmatig of *ipso facto* leidt tot de evenredigheid ervan: de pertinentie van de verwerking en van de modaliteiten moet worden aangetoond, *in casu* van de gekozen categorie en gegevens.

[74] Inzonderheid: artikel 6.1, c) van de AVG, de artikelen 44, 98 en 141 van de WGP, het Koninklijk besluit Bewapening en de omzendbrief GPI 62.
[75] Zie meer bepaald: Europees Hof voor de Rechten van de Mens, Rotaru t. Roemenië, verzoek nr. 28341/95, 4 mei 2000, §52.
[76] In de zin van artikel 9, §2, a) van de AVG.

75. Het COC wijst erop dat de verwerkingsverantwoordelijke in zijn evaluatie ook rekening moet houden met het samenvallen van de wettelijke verplichtingen die op hem rusten en van het resultaat van het dynamische risicobeheer die hij zal hebben ingevoerd. Zonder volledigheid na te streven gaat het meer bepaald om: de effectbeoordeling en risicoanalyse inzake gegevensbescherming; beleid en plan voor informatiebeveiliging; een benadering inzake welzijn op het werk die gepland en gestructureerd is en evolueert, geconcretiseerd door een beleid waarvan de toepassing is verdeeld over de verschillende bevoegdheids- en aansprakelijkheidsniveaus van de politie-entiteit; maatregelen die voortvloeien uit het risicobeheer (controle; bewustmaking; …); opleiding[77] en voorwaarden van voorafgaande toegang; informatie en preventie ten aanzien van de leden van de organisatie; technisch-preventief veiligheidsplan; enzovoort.
Er moet dus voorrang worden gegeven aan een globale benadering[78] om de maatregelen en de evenredigheid van de verwerkte gegevens te bepalen.
Het aantonen van de pertinentie van de verwerking van de vingerafdrukken ten opzichte van het beoogde doel omvat de vergelijking met de verwerking van andere afzonderlijke gegevens maar ook, in het licht van het subsidiariteitsbeginsel, en naar het oordeel van het Controleorgaan, met een combinatie van minder indringende verwerkingen van gegevens.

76. Indien er een wetgevend initiatief zou worden genomen met als doel de verwerking van biometrische gegevens mogelijk te maken voor het beheer van de toegang tot bewapening, zou de wetgever de toegevoegde waarde moeten beoordelen van de geïntegreerde uitvoering van een dergelijke verwerking, i.e. via de toepassing van eenvormige technische, organisatorische en veiligheidsmaatregelen binnen de politie-entiteiten.

[77] Ter informatie, zie de voorwaarden in het besluit Bewapening en de omzendbrief GPI 62, alsook de verplichtingen die voortvloeien uit de wet van 4 augustus 1996 betreffende het welzijn van de werknemers bij de uitoefening van hun werk, waarbij de werknemers gehouden zijn de opleiding en de door de werkgever gegeven instructies in acht te nemen (artikel 6).
[78] Een dergelijke benadering wordt overigens uitdrukkelijk aangemoedigd in de omzendbrief GPI 62 (hoofdstuk 6, deel 6). De AIG moedigt daar eveneens toe aan in haar recente verslag (Algemene Inspectie van de federale en de lokale politie, *op. cit.*, meer bepaald pp. 9, 10, 14 en 15).

OM DEZE REDENEN,

Het Controleorgaan op de politionele informatie,

Brengt uit eigen beweging het huidige advies uit

Overeenkomstig de artikelen 237 en 240, 1° en 2° van de WVG, brengt dit advies uit eigen beweging ter kennis van:

- de minister van Binnenlandse Zaken en de minister van Justitie
- de Commissaris-generaal van de gerechtelijke politie
- de Vaste Commissie van de Lokale Politie
- het Comité Informatie en ICT (art. 8*sexies* WGP)

Advies uit eigen beweging door het Controleorgaan op de politionele informatie aangenomen op 13 februari 2024.

Voor het Controleorgaan,

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