Autorité de protection des données
Gegevensbeschermingsautoriteit

Advies nr. 69/2025 van 26 augustus 2025

Betreft: advies met betrekking tot de "Nationale Cybersecurity Strategie 3.0, 2026-2030" (CO-A-2025-108)

Trefwoorden: cyberveiligheid - strategie - Centrum voor Cybersecurity België

Vertaling

Gelet op de wet van 3 december 2017 *tot oprichting van de Gegevensbeschermingsautoriteit*, met name de artikelen 23 en 26 (hierna "WOG");

Gelet op 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 "AVG");

Gelet op de wet van 30 juli 2018 *betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens* (hierna "WVG");

Gelet op de adviesaanvraag van de heer Bart De Wever, eerste minister, ontvangen op 17 juli 2025;

De Autorisatie- en Adviesdienst van de Gegevensbeschermingsautoriteit (hierna "de Autoriteit"), brengt op 26 augustus 2025 het volgende advies uit:

I. ONDERWERP EN CONTEXT VAN DE ADVIESAANVRAAG

1. De aanvrager heeft bij de Autoriteit een adviesaanvraag ingediend met betrekking tot de "Nationale Cybersecurity Strategie 3.0, 2026-2030" (hierna "**de Strategie**"), die is opgesteld door het Centrum voor Cybersecurity België (hierna "**het CCB**").

2. Artikel 28, § 1, van de wet van 26 april 2024 *tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid* (hierna "**de NIS2-wet**") bepaalt: *"De in Raad vergaderde ministers keuren de nationale cyberbeveiligingsstrategie goed en werken deze minstens om de vijf jaar bij op basis van prestatie-indicatoren,* ***na advies*** *van de Nationale Veiligheidsraad, de in artikel 15 bedoelde autoriteiten, het NCCN* ***en, in voorkomend geval, de gegevensbeschermingsautoriteiten****."* (in vet aangegeven door de Autoriteit). En overeenkomstig artikel 23, § 2, van de WOG *"[oefent] de autorisatie- en adviesdienst [...] de overige in artikel 58, § 3 van de Verordening 2016/679 bedoelde advies- en autorisatiebevoegdheden uit, uitgezonderd de bevoegdheid bedoeld in artikel 58, § 3, e) van de Verordening 2016/679"*. De onderhavige adviesaanvraag valt echter wel onder artikel 58, lid 3, van de AVG.

3. De Autoriteit benadrukt dat haar adviesbevoegdheid voornamelijk betrekking heeft op normatieve ontwerpteksten[1] en niet op teksten met een meer strategische reikwijdte, zoals de voor advies voorgelegde strategie. Dit advies zal zich dan ook **beperken tot bepaalde overwegingen met betrekking tot de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens**, zonder afbreuk te doen aan een eventueel later standpunt over de regels die op enigerlei wijze van toepassing zijn op cyberveiligheid en de verwerking van persoonsgegevens op dit gebied.

4. **De Autoriteit wijst er ook op dat haar adviezen over het algemeen om redenen van efficientie en gezien de beperkingen** waarbinnen zij haar bevoegdheid uitoefent, **zijn toegespitst op punten die in de ter advies voorgelegde projecten moeten worden verbeterd of verder uitgewerkt.** Een advies kan dus niet worden beschouwd als een uitgebreide beoordeling van het voorgelegde ontwerp. In het onderhavige geval zal de Autoriteit bijvoorbeeld niet specifiek wijzen op het belang van cyberveiligheid, waaraan de strategie gewijd is, en verwijst zij in dit verband naar de strategie zelf. Maar het is **duidelijk dat zij het algemene doel van de strategie ondersteunt**, die bovendien, zoals uit de volgende ontwikkelingen zal blijken, een synergie vormt met gegevensbescherming.

[1] Voor een specifiek geval waarin haar adviesbevoegdheid niettemin betrekking heeft op protocolakkoorden, zie artikel 9 van de wet van 21 maart 2007 *tot regeling van de installatie en het gebruik van bewakingscamera's.*

II. ONDERZOEK VAN DE STRATEGIE

Dit advies is als volgt opgebouwd:

II.1 De Autoriteit, een publieke actor op het gebied van cyberveiligheid op federaal niveau..... 3

II.2 Proactieve benadering van beveiliging en scans, analyses en continue monitoring van elektronische communicatienetwerken, in realtime..... 5

II.3. Elektronische identificatie..... 8

II.4. Encryptie en end-to-end-encryptie van elektronische communicatie.....10

II.5. Soevereiniteit 11

II.6. Evaluatie van de doeltreffendheid van de verwerking van persoonsgegevens 12

II.1 De Autoriteit, een publieke actor op het gebied van cyberveiligheid op federaal niveau

5. Allereerst wijst **de Autoriteit** de aanvrager erop dat zij **zichzelf ook beschouwt als een actor op federaal niveau met bevoegdheden en expertise op het gebied van cyberveiligheid en informatiebeveiliging in het algemeen, wanneer het gaat om de verwerking van persoonsgegevens.** Met name illustreren **artikel 32 van de AVG** (*"Beveiliging van de verwerking"*), dat de verwerkingsverantwoordelijke verplicht om passende technische en organisatorische maatregelen te treffen om een aan het risico aangepast beveiligingsniveau te waarborgen, en **de artikelen 33 en 34 van de AVG** betreffende inbreuken in verband met persoonsgegevens, duidelijk de rol van de Autoriteit op het gebied van beveiliging. Gegevensbescherming en cyberveiligheid gaan hier hand in hand.

6. Concreet betekent dit dat **het Secretariaat-Generaal van de Autoriteit** in 2024 1455 meldingen van gegevensinbreuken heeft ontvangen, waarvan er 35 zijn doorgestuurd naar de Inspectiedienst van de Autoriteit[2]. Wat betreft de meest voorkomende oorzaken van gegevensinbreuken, vertegenwoordigde de categorie *'hacking, phishing & malware"* 35% van de gemelde inbreuken[3]. Naar aanleiding van de melding van een gegevensinbreuk heeft **de Geschillenkamer** van de Autoriteit bijvoorbeeld al uitspraak gedaan in een zaak waarbij ransomware in de ziekenhuiswereld betrokken was[4].

---

[2] Zie het Jaarverslag 2024 van de Autoriteit, beschikbaar op: https://www.gegevensbeschermingsautoriteit.be/publications/jaarverslag-2024.pdf, p. 17.

[3] Ibid, p. 52. 40% houdt verband met menselijke fouten en 5% met oneigenlijk gebruik van toegangsrechten.

[4] Zie beslissing ten gronde 166/2024 van 17 december 2024, beschikbaar op: https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-166-2024.pdf (momenteel enkel beschikbaar in het Frans).

7. De **Autorisatie- en Adviesdienst** spreekt zich in zijn adviespraktijk ook uit over technische kwesties op het gebied van informatiebeveiliging en minimale gegevensverwerking[5], en is tevens bevoegd om toegang te verlenen tot metagegevens van elektronische communicatie die worden verwerkt door Belgische telecomoperatoren, door het CCB als nationaal CSIRT en door het Belgisch Instituut voor Postdiensten en Telecommunicatie (hierna "BIPT"), in het kader van de uitoefening van bepaalde taken[6]. De eerste vergunning die door de Autorisatie- en Adviesdienst aan het BIPT is afgegeven, heeft overigens betrekking op onderzoek naar de kwetsbaarheden van het SS7-protocol[7]. Op het moment van het opstellen van dit advies is ook een (nog niet gepubliceerde) eerste vergunning aan het CCB (nationaal CSIRT) afgegeven.

8. Meer in het algemeen ten slotte vallen **verwerkingen van persoonsgegevens met het oog op het waarborgen van de veiligheid van informatiesystemen onder de algemene bevoegdheid van de Autoriteit**, die er in dit verband op moet toezien dat een juist evenwicht wordt gevonden tussen de betrokken rechten en vrijheden, in overeenstemming met het Handvest van de grondrechten van de Europese Unie, de AVG, het Europees Verdrag voor de rechten van de mens en de Belgische Grondwet. Hoe legitiem zij ook moge zijn, de verwerking van persoonsgegevens die nodig is voor de in de strategie bepleite benadering van cyberveiligheid, een benadering die zowel reactief als proactief is, moet worden uitgevoerd in overeenstemming met de regels inzake gegevensbescherming.

9. Om deze redenen is **de Autoriteit van mening dat zij moet worden vermeld in de lijst van de strategie waarin de overheidsactoren op federaal niveau zijn opgenomen**, die als volgt wordt ingeleid: « *Verschillende publieke en private actoren dragen, elk vanuit hun eigen bevoegdheden en expertise, bij aan de realisatie van de missie en doelstellingen van deze cyberstrategie. De volgende entiteiten of organisaties (per categorie in alfabetische volgorde) spelen hierin een belangrijke rol op het gebied van cyberbeveiliging in ons land* »[8]. Dit sluit aan bij operationele doelstelling nr. 1, onder de titel *"BEHEREN"* van de Strategie: « *Een duidelijk overzicht van rollen en verantwoordelijkheden op*

---

[5] Zie bijvoorbeeld, Gegevensbeschermingsautoriteit, Autorisatie- en Adviesdienst, "De adviespraktijk van de Autorisatie- en Adviesdienst, publieke sector en wettelijke verplichtingen", 01/09/2024, beschikbaar op https://www.gegevensbeschermingsautoriteit.be/publications/brochure-publieke-sector-en-wettelijke-bepalingen.pdf, pp. 57, 60-67. Meer recent, zie met name betreffende een protocol voor realtimetoegang tot bewakingscamera's, advies nr. 118/2027 van 23 december 2024 *over een protocolakkoord tot regeling van de realtimetoegang van de federale politie tot de beelden van de camera's die zijn geïnstalleerd op het net van de NMBS* (CO-A-2024-268), punten nr. 67 e.v., zie ook voetnoot nr. 15.

[6] Zie artikel 21, § 2, van de wet van 26 april 2024 *tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid* betreffende het CCB (Nationaal CSIRT), en artikel 15 van de wet van 17 januari 2003 *betreffende het statuut van de regulator van de Belgische post- en telecommunicatie*.

[7] Zie (afgeleverde) vergunning nr. 001/2024 van 6 november 2024 *betreffende een aanvraag tot vergunning bedoeld in artikel 15, § 2, tweede lid, van de wet van 17 januari 2003 betreffende het statuut van de regulator van de Belgische post- en telecommunicatie (AH-2024-0010).*

[8] Strategie, pp. 32-33. De lijst van overheidsactoren op federaal niveau omvat 22 entiteiten, waaronder Belnet, de federale politie, de FSMA, de Nationale Bank, het FAGG, het BIPT, de FOD BOSA, de FOD Economie en natuurlijk het CCB zelf.

het gebied van cyberbeveiliging definiëren en onderhouden ». Met name **ziet de Autoriteit toe op de beveiliging van de verwerking van persoonsgegevens**.

II.2 Proactieve benadering van beveiliging en scans, analyses en continue monitoring van elektronische communicatienetwerken, in realtime

10. Ten tweede merkt de Autoriteit op dat de ontwikkelde strategie sterk de nadruk legt op een **proactieve benadering van cyberveiligheid en op de daarmee samenhangende noodzaak om bedreigingen** snel te identificeren, zodat zo snel mogelijk passende tegenmaatregelen kunnen worden genomen. Deze aanpak is met name gebaseerd op de noodzaak van **scans, analyses en continue monitoring van netwerken in realtime**, waardoor bedreigingen beter zichtbaar worden. Kortom, het gaat om een **versterkte activiteit op het vlak van toezicht, verzameling en uitwisseling van informatie en gegevens, met als doel een betere cyberveiligheid in België te verzekeren**.

11. Deze aanpak komt in de hele strategie naar voren. De volgende fragmenten uit de operationele doelstellingen (in vet aangegeven door de Autoriteit) illustreren dit duidelijk:

- Doelstelling nr. 8 (« *Extend Early Warning Systems* »): punt II., waarin de operationele doelstellingen nrs. 8 tot en met 10 zijn opgenomen, bepaalt met name: « *Door **realtime informatie, continue monitoring en mechanismen voor het delen** van bedreigingen te integreren, kunnen organisaties overschakelen van een reactieve houding naar een proactieve cybersecurity strategie*. »

- Doelstelling nr. 9 (« *Het scannen, analyseren en delen van informatie over kwetsbaarheden versterken* »): « *Door de Belgische capaciteiten voor **het scannen** van kwetsbaarheden, analyse en **het delen van informatie** te versterken, kunnen we onze **zichtbaarheid** in onze meest kritieke kwetsbaarheden aanzienlijk verbeteren. Door digitaal België **beter te scannen op nationaal niveau** zal het CCB, samen met nationale en internationale partners, eigen **informatie over cyberdreigingen (CTI) verzamelen en produceren** die grondig kan worden geanalyseerd. Het doel is om kwetsbare systemen te identificeren en **hun eigenaars rechtstreeks te waarschuwen**, niet alleen van NIS2-entiteiten, maar **van alle organisaties in België**. Dit zal resulteren in **het delen van betere en gerichte informatie**, bekend als "Spear Warnings," een bedacht door het CCB*. »

- Doelstelling nr. 11 (« *Verminder e-fraude : een nationale noodzaak* »): « *Effectieve en efficiente maatregelen zijn essentieel voor dit initiatief. Ten eerste moet **de verzameling van***

informatie *over (potentiële) fraude worden* ***gestroomlijnd tussen alle betrokken partijen*** *om een volledige gegevensvergaring te garanderen* »;

- Doelstelling nr. 18 (« *Efficiënte AI-gestuurde dreigingsdetectiemechanismen implementeren* »): « *Het CCB zal efficiënte* ***AI-gestuurde dreigingsdetectiemechanismen*** *implementeren om voorop te blijven lopen op cyberdreigingen in het snel evoluerende digitale landschap van vandaag. Het doel is om* ***sneller verdachte activiteiten te identificeren,*** *de responstijden te verkorten en mogelijke schade te minimaliseren* ***door continu netwerkverkeer te monitoren en analyseren***. »

- Doelstelling nr. 19 (« *Netwerkverkeer op indicatoren van bedreigingen monitoren en analyseren* »): « *De* ***monitoring en analyse van mogelijk kwaadaardig netwerkverkeer*** *zullen worden verbeterd om* ***dreigingsindicatoren in bijna real-time te identificeren****. Het CCB zal samenwerken met de relevante partners en het bestaande wettelijke kader implementeren. Het doel is om potentiële cyberdreigingen* ***snel te detecteren en erop te reageren,*** *waardoor de integriteit en veiligheid van de digitale infrastructuur van België wordt gewaarborgd* »; « *Door* ***mogelijk kwaadaardig netwerkverkeer te monitoren en analyseren****, kunnen we deze communicatie ontdekken, de acties van de aanvaller analyseren, nieuwe kwaadaardige servers* ***detecteren*** *en nieuwe slachtoffers* ***identificeren*** *die zich mogelijk nog niet bewust zijn dat ze zijn gecompromitteerd. Deze* ***proactieve benadering*** *is cruciaal voor het handhaven van een robuuste cyberweerbaarheid*. »

- Doelstelling nr. 20 (« *Nauw samenwerken met cloudserviceproviders om de zichtbaarheid en responsmogelijkheden te verbeteren* »): « *Het CCB blijft prioriteit geven aan* ***samenwerking met CSP's*** [9]*, waarbij cloudservices worden erkend als kritieke digitale activa. Dit partnerschap levert tastbare voordelen op, waaronder verbeterde beveiliging door* ***realtime dreigingsdetectie****, robuuste encryptie en gelaagde toegangscontroles* »; « *Bovendien verbetert de samenwerking met CSP'sde* ***zichtbaarheid van gegevens****, risicobeheer en naleving, terwijl het* ***geavanceerde analyses en monitoring*** *mogelijk maakt voor betere besluitvorming*. »

- Doelstelling nr. 21 (« *Toegang tot duidelijk kwaadaardige infrastructuur blokkeren* »): « *De infrastructuur die door aanvallers wordt gebruikt, is cruciaal voor het succes van cyberaanvallen. Door toegang tot deze infrastructuur te blokkeren, kunnen we onmiddellijk invloed uitoefenen op lopende aanvallen en hun effectiviteit verminderen. Dit vereist het in kaart brengen van kwaadaardige infrastructuur* ***door middel van diepgaande CyberThreat Intelligence***

[9] Cloudserviceproviders.

(CTI) verzamelingen analyse, *zodat we weten wat we moeten blokkeren. Deze* ***proactieve maatregel*** *is essentieel voor het handhaven van een robuuste cyberweerbaarheid*. »

- En ten slotte doelstelling nr. 23 (« *Verstoring door cyberincidenten minimaliseren* »): « *Om de continuiteit van essentiële diensten te waarborgen, is een proactieve en gecoordineerde aanpak nodig waarmee* ***dreigingen snel kunnen worden geïdentificeerd en geneutraliseerd voordat ze escaleren*** »; « *Om de veerkracht verder te vergroten, zal het CCB zijn incidentresponsteam versterken met een dubbele focus op reactieve* ***en proactieve capaciteiten****, waaronder het opsporen van bedreigingen, veiligheidsbeoordelingen en technische adviesdiensten. Deze evolutie van incidentafhandeling naar een volledige responscapaciteit zal de* ***detectiesnelheid aanzienlijk verbeteren*** *en de hersteltijd verkorten*. »

12. De Autoriteit gaat ervan uit dat de eerste aanvraag tot vergunning die haar door het CCB (nationaal CSIRT) is toegezonden, in dit kader werd ingediend, namelijk om bij telecommunicatie-exploitanten de metadata te verzamelen van alle elektronische communicatie die heeft plaatsgevonden van en naar IP-adressen die zijn opgenomen in lijsten die zijn gewijd aan het verkeer van kwaadaardige *Command-and-Control-servers* of C2-servers. Het doel is om op basis hiervan potentiële slachtoffers te identificeren en hen vervolgens te waarschuwen. Of deze slachtoffers nu wel of niet essentiële of belangrijke entiteiten zijn die onderworpen zijn aan de verplichtingen van de NIS2-wet. In deze vergunning heeft de Autoriteit met betrekking tot het concrete project benadrukt dat de wetgever zou moeten bevestigen dat het inderdaad zijn bedoeling was om de verwerking van metagegevens van deze entiteiten of personen die niet essentieel of belangrijk zijn in de zin van de NIS2-wet toe te staan, omdat dit minder duidelijk – en dus voorspelbaar – is gezien de bepalingen van de NIS2-wet.

13. In deze context is de Autoriteit van mening dat **de strategie ook,** voor zover mogelijk**, meer concrete zichtbaarheid moet bieden over wat het toezicht, de continue monitoring en de realtimeanalyse van openbare elektronische communicatienetwerken** (geleverd door telecommunicatie-exploitanten) **of particuliere elektronische communicatienetwerken** (clouddienstverleners, bedrijven, enz.)**, zoals beoogd door het CCB, precies inhoudt,** zodat er een beter inzicht kan worden verkregen in de **verwerking van persoonsgegevens** (verzameling, uitwisseling, enz.) **die hiervoor nodig is**.

14. Zij vestigt ook de aandacht van de aanvrager op **het belang, bij de uitvoering van de strategie, van het onderscheid tussen enerzijds preventie- en beschermingsactiviteiten van puur technische** (en "civiele") **aard** (het gaat erom zichzelf te beschermen en technische maatregelen te nemen die de impact van de betrokken bedreigingen beperken of verhinderen) en **anderzijds activiteiten op het gebied van onderzoek en bestraffing van inbreuken door de bevoegde autoriteiten**, of het nu gaat om het bestraffen van inbreuken in verband met schendingen van de NIS2-

wet, cybercriminaliteit of, meer in het algemeen, elke andere inbreuk die door het CCB bij de uitoefening van zijn taken wordt ontdekt. Het CCB kan namelijk, afhankelijk van zijn bevoegdheden en de wijze waarop deze worden uitgeoefend, bevoorrechte toegang hebben tot openbare netwerken (van exploitanten) en particuliere netwerken van (essentiële of belangrijke, of andere) entiteiten.

15. Ten slotte vermeldt doelstelling nr. 18 (« *Efficiënte AI-gestuurde dreigingsdetectiemechanismen implementeren* ») die reeds ter sprake is gebracht in punt nr. 11 ook: « *Het implementeren van AI-gestuurde dreigingsdetectie als een nationale CSIRT omvat snelle en efficiënte diagnose tijdens incidenten,* ***continue monitoring, data-analyse en geautomatiseerde reacties***. » (in vet aangegeven door de Autoriteit). Zonder hier in detail te treden over de recente Europese regelgeving inzake **artificiële intelligentie**[10], herinnert de Autoriteit eraan dat **artikel 22 van de AVG** de mogelijkheden beperkt om een besluit te nemen ten aanzien van een betrokkene dat uitsluitend is gebaseerd op geautomatiseerde gegevensverwerking, waaronder profilering, waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft[11]. Er kan **een specifiek normatief kader** nodig zijn op dit gebied indien een dergelijk scenario wordt overwogen bij de uitvoering van de strategie.

II.3. Elektronische identificatie

16. De strategie gaat in op het onderwerp **elektronische identificatie** en zegt hierover met name het volgende:

> « *In België is het vanzelfsprekend dat* ***de overheid instaat voor het beheer van onze fysieke identiteit****, bijvoorbeeld via en identiteitskaarten.* ***Diezelfde willen we doortrekken de digitale wereld: het waarborgen van digitale identiteit*** *op een manier die betrouwbaar,* ***publiek gestuurd*** *en veilig is — zonder afhankelijk te zijn van buitenlandse, vaak niet-Europese technologiebedrijven. Nu reeds wordt in ons land toegang tot gevoelige informatie voornamelijk geregeld via een publiek-private samenwerkingen dit willen we verder zetten.*
>
> *Het uitgangspunt is duidelijk: er moet vermeden worden dat we evolueren naar een digitale samenleving waarin grote technologiebedrijven volledige controle uitoefenen over hoe we ons online identificeren en gedragen.*

[10] Verordening (EU) 2024/1689 van het Europees Parlement en de Raad van 13 juni 2024 *tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie en tot wijziging van de Verordeningen (EG) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 en (EU) 2019/2144, en de Richtlijnen 2014/90/EU, (EU) 2016/797 en (EU) 2020/1828 (verordening artificiële intelligentie)*.

[11] Zie ook "De adviespraktijk van de Autorisatie- en Adviesdienst, Publieke sector en wettelijke verplichtingen", pp. 46-48, waarnaar wordt verwezen in voetnoot nr. 5.

> *Tegelijk **is het cruciaal dat ook overheidsoplossingen geen systeem worden waarmee het gedrag van burgers systematisch kan worden gemonitord**. Een volledig anonieme samenleving is echter niet realistisch of veilig. Hoewel we in het dagelijks leven meestal anoniem kunnen blijven, zijn er situaties waarin identificatie noodzakelijk is; denk aan het openen van een bankrekening of het nemen van een vlucht.* » (in vet aangegeven door de Autoriteit).

17. De Autorisatie- en Adviesdienst heeft zich vrij recentelijk uitgesproken op het gebied van elektronische identificatie waarbij met name werd verwezen naar Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 *betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (hierna "eIDAS-verordening")*, zoals gewijzigd door Verordening (EU) 2024/1183 van het Europees Parlement en de Raad van 11 april 2024 *tot wijziging van Verordening (EU) nr. 910/2014, wat betreft de vaststelling van het Europees kader voor digitale identiteit* [12](hierna "**eIDAS-verordening**"), en naar **de Europese portemonnee voor digitale identiteit**.

18. De Autoriteit benadrukt in dit verband dat identificatie weliswaar betrouwbaar moet zijn, maar **alleen mag worden vereist wanneer dat noodzakelijk is en voor zover het noodzakelijk is** overeenkomstig het beginsel van minimale gegevensverwerking, **in het licht van het nagestreefde doel**. Er zijn heel vaak situaties waarin de identificatie van de betrokkenen online niet nodig is, ongeacht het gebruikte identificatiemiddel of de gebruikte identificatiedienst (door de staat of een andere instantie verstrekt). Het is ook mogelijk dat slechts één attribuut moet worden geverifieerd, dat een e-mailadres, een wachtwoord en een tweede identificatiefactor volstaan, enz. De eIDAS-verordening zelf voorziet in verschillende vertrouwensniveaus voor elektronische identificatie. Voor een gemiddelde gebruiker kan online anonimiteit bovendien ook relatief zijn, gezien de vele sporen die hij achterlaat (moet achterlaten), afhankelijk van de gebruikte technologie en de informatie die wordt verzameld door de verschillende betrokken dienstverleners, de aanwezigheid van een financiële transactie, enz. In een dergelijke context mag de identificatieverplichting ook niet worden gebruikt om onnodige gegevens over de betrokkenen te verzamelen.

19. Op dit gebied zijn enerzijds **de controle en de autonomie van de betrokkene over zijn identificatie doorslaggevend**. Dit uiteraard **zonder afbreuk te doen aan de wettelijke identificatieverplichtingen** die gelden in bepaalde specifieke gereglementeerde sectoren, zoals de in de strategie genoemde banksector; wettelijke verplichtingen die z**elf moeten waarborgen dat** onder meer **de beginselen van doelbinding en evenredigheid worden toegepast.** Anderzijds is het, zoals

[12] Zie advies nr. 14/2025 van 27 februari 2025 *betreffende een wetsvoorstel tot delen van data uit authentieke bronnen met erkende dienstverleners voor elektronische identificatiemiddelen (DOC560330/001) en een daarmee verband houdend amendement (DOC56 0330/002) (CO-A-2025-003)*.

de strategie terecht benadrukt, **van cruciaal belang dat identificatieoplossingen in het algemeen niet kunnen worden gebruikt om de activiteiten van de betrokkenen te monitoren**. Zo legt de eIDAS-verordening verplichtingen in die zin vast met betrekking tot Europese digitale identiteitsportefeuilles en voorziet zij in *"volledige controle"* van de betrokkene over de hem betreffende gegevens[13].

II.4. Encryptie en end-to-end-encryptie van elektronische communicatie

20. Operationele doelstelling nr. 16 heeft betrekking op **encryptie, in het bijzonder in verband met kwantumcomputers** (« *Aan een kwantumveilige en flexibele cryptografie / toekomstbestendige beveiliging bijdragen* »)[14]. In deze context: « *De CCB zal de ontwikkeling en verspreiding van een nationaal cryptografiebeleid, een roadmap en richtlijnen voor niet-geclassificeerde gegevens coördineren, in nauwe samenwerking met, en op basis van input van, de nationale, regionale en internationale contextpartners* ».

21. In dit verband heeft de Autoriteit in een recent advies het belang benadrukt van het behoud van end-to-end-encryptie van elektronische communicatie[15] en maakt zij van de gelegenheid gebruik om in dit advies nogmaals op dit punt te wijzen. Zonder hier opnieuw in te gaan op de gedetailleerde overwegingen ter zake in het bovengenoemde advies waarnaar wordt verwezen, kan een uittreksel van het standpunt van het Europees Comité voor gegevensbescherming zelf worden weergegeven: « *the EDPB stresses again* [EDPB-EDPS Joint Opinion 4/2022 and EPDB Statement 1/2024] *that encryption is* ***essential for ensuring the security and confidentiality of personal data and electronic communications****, as it provides strong technical safeguards against access to that information by anyone other than the user and the recipients chosen by him, including by the provider. In particular, in the context of interpersonal communications, genuine end-to-end encryption ('E2EE') covering the terminal devices and the data therein, with the decryption keys held solely by the users is a crucial tool for ensuring the confidentiality of electronic communications.* ***Preventing the use of encryption or weakening the effectivity of the protection it provides, would have a severe impact on the respect for private life and confidentiality of users, on their freedom of expression as well***

Zie artikel 5bis, 1., 4., a), b), 14, 15 en 16 van de eIDAS-verordening.

[14] In dit verband zie met name:
https://www.nist.gov/cybersecurity/what-post-quantum-cryptography;
https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards;
laatstelijk geraadpleegd op 31/07/2025.

[15] Zie advies nr. 16/2025 van 27 maart 2025 *uit eigen beweging betreffende het Verdrag van de Verenigde Naties tegen cybercriminaliteit (CO-A-2025-019)*.

as on innovation and the growth of the digital economy, which relies on the high level of trust and confidence that such technologies provide »[16] (in vet aangegeven door de Autoriteit).

22. De strategie zou ook kunnen wijzen op de **centrale rol van end-to-end-encryptie van elektronische communicatie** op het gebied van cyberbeveiliging (vertrouwelijkheid) en de daarmee samenhangende noodzaak om de **goede werking ervan te behouden en te waarborgen**.

II.5. Soevereiniteit

23. Operationele doelstelling nr. 17 heeft betrekking op de **soevereiniteit** (« *Voor een Soevereine cloud zorgen en de soevereiniteit van gegevens waarborgen* ») en bepaalt met name: « *Het CCB werkt samen met nationale partners aan* ***de ontwikkeling van een Soevereine Cloud*** *als strategische prioriteit om de nationale digitale autonomie te waarborgen,* ***gegevenssoevereiniteit te garanderen en de afhankelijkheid van niet-EU cloudserviceproviders te verminderen****. In een tijdperk waarin cloud computing zowel publieke als sectoractiviteiten ondersteunt, is het essentieel om* ***controle te behouden over gevoelige gegevens binnen de jurisdictie van de EU om privacy te beschermen, naleving van regelgeving te waarborgen en nationale belangen te beschermen****. Dit initiatief integreert regelgevende, operationele en technische dimensies binnen een uniform controle en governance kader. Het waarborgt regelgevende soevereiniteit door afstemming op nationale en EU wetgevingskaders, inclusief transparante gegevensverwerking, beperkte buitenlandse invloed en volledige zichtbaarheid op (sub)verwerkers en metadataflows* » (in vet aangegeven door de Autoriteit).

24. De Autoriteit is van mening dat een dergelijke aanpak **positieve effecten kan hebben op het gebied van de bescherming van betrokkenen** met betrekking tot de verwerking van persoonsgegevens, ofschoon de wettelijke regeling voor grensoverschrijdende gegevensstromen in de AVG bijdraagt tot het beperken van de risico's voor betrokkenen in de internationale omgeving buiten de Unie. **Het feit dat de gegevensverwerking uitsluitend onder de bevoegdheid van de lidstaten van de Europese Economische Ruimte valt, garandeert een grotere doeltreffendheid van de Europese normen inzake gegevensbescherming.**

[16] EDPB, « Statement 5/2024 on the Recommendations of the Hight-Level Group on Access to Data for Effective Law Enforcement », vastgesteld op 4 november 2024, punt nr. 3, beschikbaar op https://www.edpb.europa.eu/system/files/2024-11/edpb_statement_20241104_ontherecommendationsofthehlg_en.pdf, laatstelijk geraadpleegd op 30/07/2025.

II.6. Evaluatie van de doeltreffendheid van de verwerking van persoonsgegevens

25. Ten slotte bepaalt de strategie[17]: « *Het Centrum voor Cybersecurity België (CCB) zal een reeks* ***prestatie-indicatoren ontwikkelen om de voortgang en effectiviteit van de Nationale Cybersecurity Strategie te meten****. De indicatoren zullen* ***kwantitatieve en kwalitatieve metingen omvatten*** *die toelaten om de evolutie naar de strategische objectieven in kaart te brengen. Jaarlijks zal het CCB een gedetailleerd rapport opstellen waarin de prestaties op basis van deze indicatoren worden geëvalueerd. Dit rapport zal een analyse bevatten van de behaalde resultaten, geïdentificeerde tekortkomingen, en aanbevelingen voor verbeteringen. Het rapport zal worden voorgelegd aan de regering, die op basis van de bevindingen de uitvoering van de strategie kan bijsturen*. » (in vet aangegeven door de Autoriteit).

26. De Autorisatie- en Adviesdienst heeft al aanbevolen om een **mechanisme in te voeren voor de evaluatie van de doeltreffendheid van de verwerkingen van persoonsgegevens** waarin bepaalde wetgevingen voorzien, nadat deze verwerkingen zijn uitgevoerd, bijvoorbeeld door middel van de opstelling en publicatie van specifieke statistieken en evaluatieverslagen, waarmee de wettigheid, doeltreffendheid en evenredigheid van het betrokken systeem en de uitvoering ervan kunnen worden aangetoond[18]. Dit is onder andere gebeurd in het kader van het bewaren van metagegevens van elektronische communicatie, op het gebied van de identificatie van de eindgebruiker van openbaar toegankelijke elektronische communicatiediensten die op basis van een prepaidkaart worden geleverd, en in het kader van het gebruik van bewakingscamera's.

27. Het is belangrijk dat de indicatoren die worden gebruikt om de uitvoering van de strategie te evalueren, betrekking hebben op **de doeltreffendheid van de maatregelen en controlesystemen die in het kader van de strategie worden toegepast, met name wat betreft de verwerking van metagegevens van elektronische communicatie en identificatiegegevens** van gebruikers van elektronische communicatiediensten. Op die manier kan met name worden aangetoond dat de uitgevoerde verwerkingen van persoonsgegevens hun doel effectief bereiken.

---

[17] Blz. 29.

[18] Zie "De adviespraktijk van de Autorisatie- en Adviesdienst, Publieke sector en wettelijke verplichtingen", pp. 25 en 44, waarnaar wordt verwezen in voetnoot nr. 5, en advies nr. 16/2025, punten nrs. 18 en 19, waarnaar wordt verwezen in voetnoot nr. 15.

OM DEZE REDENEN,

is de Autoriteit van mening dat, binnen de grenzen zoals vermeld in de punten nrs. 3-4:

1. Zij zou moeten worden vermeld in de lijst van de strategie waarin de overheidsactoren op federaal niveau zijn opgenomen, aangezien zij ook een actor op federaal niveau is met bevoegdheden en expertise op het gebied van cyberveiligheid en informatiebeveiliging in het algemeen wanneer het gaat om de verwerking van persoonsgegevens (**punten nrs. 5-9**);

2. De strategie moet, voor zover mogelijk, een concreter beeld geven van het toezicht, de continue monitoring en de realtime analyse van openbare elektronische communicatienetwerken (geleverd door telecommunicatie-exploitanten) of particuliere netwerken (clouddienstverleners, bedrijven, enz.) die door het CCB worden overwogen, zodat er een beter inzicht kan worden verkregen in de verwerkingen van persoonsgegevens (verzameling, uitwisseling, enz.) die hiervoor nodig zijn. Bij de uitvoering van de strategie is het belangrijk om een onderscheid te maken tussen preventie- en beschermingsactiviteiten van puur technische (en "civiele") aard (het gaat erom zichzelf te beschermen en technische maatregelen te nemen die de impact van de betreffende bedreigingen beperken of verhinderen) en activiteiten op het gebied van onderzoek en bestraffing van inbreuken door de bevoegde autoriteiten. Artikel 22 van de AVG kan bij de uitvoering van de strategie, afhankelijk van de overwogen scenario's, een specifiek normatief kader vereisen (**punten nrs. 10-15**);

3. Elektronische identificatie mag alleen worden opgelegd wanneer en voor zover dat noodzakelijk is. De betrokkene moet de controle over zijn identificatie behouden, onverminderd de toepasselijke normatieve verplichtingen op het gebied van identificatie. En de diensten en middelen die in dit verband ter beschikking worden gesteld, mogen niet leiden tot monitoring van de activiteiten van de betrokkenen, zoals ook in de strategie wordt benadrukt (**punten nrs. 16-19**);

4. De strategie zou ook kunnen wijzen op de centrale rol van end-to-end-encryptie van elektronische communicatie op het gebied van veiligheid (vertrouwelijkheid) en de daarmee samenhangende noodzaak om de goede werking ervan te behouden en te waarborgen (**punten nrs. 20-22**);

5. De ontwikkeling van een soevereine cloud kan daadwerkelijk bijdragen tot en zorgen voor de effectieve toepassing van de Europese normen op het gebied van de bescherming van personen met betrekking tot de verwerking van persoonsgegevens (**punten nrs. 23-24**);

6. Het is belangrijk dat de indicatoren die worden gebruikt om de uitvoering van de strategie te evalueren, betrekking hebben op de doeltreffendheid van de maatregelen en controlesystemen die in het kader van de strategie worden toegepast, met name wat betreft de verwerking van metagegevens van elektronische communicatie en identificatiegegevens van gebruikers van elektronische communicatiediensten. Op die manier kan met name worden aangetoond dat de uitgevoerde verwerkingen van persoonsgegevens hun doel effectief bereiken (overwegingen nrs. **25-27**).

Voor de Autorisatie- en Adviesdienst,
(get.) Alexandra Jaspar, directeur