



Autorité de protection des données
Gegevensbeschermingsautoriteit

Advies nr. 41/2025 van 12 juni 2025

Betreft: adviesaanvraag met betrekking tot een ontwerp van bilateraal Verdrag betreffende wederzijdse rechtshulp in strafzaken tussen het Koninkrijk België en de Republiek Kosovo (CO-A-2025-026)

Trefwoorden: doorgiften van gegevens buiten de EU – internationaal verdrag – wederzijdse strafhulp in strafzaken – Kosovo – Richtlijn 2016/680 – titel II WVG

Vertaling

De Autorisatie- en Adviesdienst van de Gegevensbeschermingsautoriteit (hierna "de Autoriteit");

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 met betrekking tot de verwerking van persoonsgegevens* (hierna "WVG");

Gelet op de adviesaanvraag van mevrouw Annelies Verlinden, minister van Justitie (hierna "de aanvrager"), ontvangen op 28 maart 2025;

Gelet op de e-mail van het Controleorgaan op de politionele informatie van 17 april 2025, waarin wordt aangegeven dat het geen advies zal uitbrengen over dit ontwerp;

Brengt op 12 juni 2025 het volgende advies uit:

Voor normatieve teksten die uitgaan van de federale overheid, het Brussels Hoofdstedelijk Gewest en de Gemeenschappelijke Gemeenschapscommissie zijn de adviezen in principe zowel in het Nederlands als in het Frans beschikbaar op de website van de Autoriteit. De 'Originale versie' is de versie die gevalideerd werd.

I. VOORWERP VAN DE ADVIESAANVRAAG

1. De aanvrager heeft het advies van de Autoriteit gevraagd over artikel 7 van het ontwerp van Verdrag betreffende wederzijdse rechtshulp in strafzaken (hierna "het ontwerp").
2. Bij de indiening van de adviesaanvraag verduidelijkte de afgevaardigde ambtenaar dat de aanvraag werd ingediend vóór de ondertekening van het ontwerp van Verdrag door de bevoegde minister. De Autoriteit neemt hiervan akte en¹ erkent dat, wanneer internationale verdragen verwerkingen van persoonsgegevens met zich meebrengen, het raadplegen van de Autoriteit vóór de ondertekening van het betreffende verdrag beter toelaat om een doeltreffende bescherming van de rechten van de betrokkenen te waarborgen². Bijgevolg, onverminderd de noodzaak om het ontwerp van instemmingswet ter advies voor te leggen aan de Autoriteit, aanvaardt de Autoriteit (voor zover zij daartoe materieel in staat is) zich uit te spreken over een ontwerp van internationaal verdrag dat België kan binden, voorafgaand aan de ondertekening ervan door de partijen.
3. Het ontwerp beoogt de partijen in staat te stellen elkaar wederzijdse rechtshulp te verlenen in het kader van een strafrechtelijk onderzoek of een strafrechtelijke procedure, en meer bepaald bij de uitvoering van onderzoekshandelingen (verhoren, huiszoekingen, inbeslagnemingen, verzoeken om inlichtingen), de uitvoering van proceshandelingen in verband met een strafrechtelijke procedure (betekeningen), de uitwisseling van strafregisters en de spontane uitwisseling van informatie³.
4. In het adviesaanvraagformulier wordt vermeld dat – onder bepaalde voorwaarden – samenwerking tussen Kosovo en België in het kader van wederzijdse rechtshulp in strafzaken reeds mogelijk is op basis van de [Overeenkomst](#) van [1971]⁴ betreffende uitlevering en wederzijdse rechtshulp in strafzaken tussen het Koninkrijk België en de Socialistische Federatieve Republiek Joegoslavië voor wat betreft wederzijdse rechtshulp, multilaterale verdragen van de Verenigde Naties en wederkerigheid⁵.

¹ Niettegenstaande artikel 46, § 1, van het Reglement van interne orde van de Autoriteit, dat het volgende bepaalt: "[...] *de [AAD] [behandelt] alleen adviesaanvragen over normatieve ontwerpen (...) die zich in hun finale ontwerpfasen bevinden*".

² Zie in die zin advies 119/2022 van 15 juni 2022, punt 7; zie ook punt 48 van de Guidelines [01/2023](#) on Article 37 Law Enforcement Directive van de EDPB, waarin het volgende staat: "*In any case, Member States are in all circumstances encouraged to **engage with the national SA before the conclusion of the legally binding agreement** to allow for a timely, constructive and meaningful exchange in order to verify that the appropriate safeguards are in place, in line with the requirements of Article 37(1)(a) LED. In that context, the SA should be provided with all relevant information regarding the third country or international organisations, including the respective assessments made, when available.*"

³ Art. 10 e.v. van het ontwerp.

⁴ Het adviesaanvraagformulier vermeldt "1970".

⁵ Wat politiegegevens betreft, moet worden opgemerkt dat Kosovo geen lid is van Interpol (zie <https://www.kosovo-online.com/en/news/politics/dacic-it-serbias-interest-kosovo-does-not-join-interpol-13-5-2025>).

5. De strafrechtelijke context waarin de beoogde verwerkingen van persoonsgegevens plaatsvinden, brengt de toepassing mee van hoofdstuk V van Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 *betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad* (hierna "Richtlijn politie-justitie"), zoals omgezet in Belgisch recht bij hoofdstuk V van titel 2 van de WVG.
6. Tot op heden is Kosovo door de Europese Commissie niet erkend als een land met een passend beschermingsniveau⁶. Persoonsgegevens mogen dus alleen aan Kosovo worden doorgegeven als⁷ het land een voldoende niveau van bescherming van de persoonlijke levenssfeer en de fundamentele rechten en vrijheden van personen waarborgt met betrekking tot de verwerking van die gegevens, zoals bepaald in artikel 66, § 1, van de WVG.
7. De Autoriteit onderzoekt hierna of het ontwerp voldoet aan de voorwaarden om te worden beschouwd als een juridisch bindend instrument dat passende waarborgen biedt voor de bescherming van persoonsgegevens die kunnen worden doorgegeven aan derde landen buiten de Europese Unie, overeenkomstig artikel 68, § 1, 1°, van de WVG⁸.
8. Er zij opgemerkt dat Kosovo – dat in februari 2008 eenzijdig zijn onafhankelijkheid heeft uitgeroepen – een potentiële kandidaat is voor toetreding tot de Europese Unie. Artikel 36 van de Kosovoarse Grondwet beschermt de persoonlijke levenssfeer en waarborgt de bescherming van persoonsgegevens⁹. Sinds 13 februari 2019¹⁰ is in Kosovo specifieke wetgeving inzake gegevensbescherming van toepassing (die de bepalingen van de AVG "omzet"¹¹). Bovendien beschikt het land

⁶ Artikel 36 van Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 verleent de Commissie de bevoegdheid om bij besluit vast te stellen dat een derde land een adequaat beschermingsniveau verzekert (zie ook artikel 67 van de WVG en natuurlijk artikel 45.1 van de AVG).

⁷ Naast, in strafrechtelijke context, de voorwaarde dat de doorgifte noodzakelijk is "met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid" (artikel 27 van de WVG).

⁸ Evenals artikel 37 van de bovengenoemde Richtlijn politie-justitie.

⁹ Zie <https://qzk.rks-gov.net/ActDetail.aspx?Ac-tID=3702>.

¹⁰ Zie <https://www.dlapiperdataprotection.com/?t=law&c=XK>.

¹¹ De bepalingen die van toepassing zijn op gerechtelijke procedures en het strafregister zijn echter voornamelijk opgenomen in wet [No.05/L-053 ON SPECIALIST CHAMBERS AND SPECIALIST PROSECUTOR'S OFFICE](#) en wet [No. 08/L-194 ON CENTRAL CRIMINAL RECORDS SYSTEM OF KOSOVO](#).

over een onafhankelijke gegevensbeschermingsautoriteit¹². Deze autoriteit heeft binnen de EDPB de status van waarnemer¹³.

9. De Autoriteit maakt van de gelegenheid gebruik om erop te wijzen dat de Belgische wetgever tot op heden nog steeds niet heeft bepaald welke autoriteit bevoegd is voor het toezicht op de verwerking van persoonsgegevens door de hoven en rechtbanken, alsook door het Openbaar Ministerie, in het kader van hun gerechtelijke taken.
10. Tot slot merkt de Autoriteit voor de goede orde op dat een andere lidstaat van de Unie (Zweden) onlangs een verdrag betreffende uitlevering, een verdrag betreffende wederzijdse rechtshulp in strafzaken, en een verdrag betreffende overbrenging van veroordeelden met Kosovo heeft ondertekend¹⁴.

II. ONDERZOEK VAN HET ONTWERP

11. Artikel 7 in ontwerp heeft betrekking op de "*bescherming van persoonsgegevens*"¹⁵. Bij de indiening van de adviesaanvraag heeft de afgevaardigde ambtenaar de Autoriteit gevraagd haar onderzoek tot deze ene bepaling te beperken. Zoals hieronder nader zal worden toegelicht, hebben andere bepalingen van het ontwerp echter ook duidelijk betrekking op de verwerking van persoonsgegevens.

¹² Die slechts 19 medewerkers telde in 2019 (zie Hajdari, P., Nimani, P., Hebibi, D., & Maloku, A. (2022). Implementation of the right to privacy in the Republic of Kosovo. *International Journal of Health Sciences*, 6(S8), p. 5037 (<https://doi.org/10.53730/ijhs.v6nS8.13358>) en 32 in 2024 (zie het [jaarverslag van 2024](#) van de AIP van Kosovo, p. 15).

¹³ Zie <https://idp.al/en/2024/10/11/information-and-privacy-agency-of-kosovo-member-of-the-european-data-protection-board/>.

¹⁴ Zie <https://kosovapress.com/kosova-e-suedia-finalizojne-tri-marreveshie-per-bashkepunim-juridik>.

¹⁵ En luidt als volgt:

1. De Partijen zien erop toe dat de persoonsgegevens die door de ene Partij aan de andere worden overgedragen, uitsluitend dienen **voor de uitvoering van een verzoek** volgens deze Overeenkomst. Persoonsgegevens mogen niet voor andere doeleinden worden gebruikt en niet aan derde landen worden overgedragen zonder voorafgaande toestemming van de Partij die ze overdragen.

2. De Partijen waarborgen de **juistheid** van de in het kader van deze Overeenkomst overgedragen persoonsgegevens en zien erop toe dat er passende maatregelen worden genomen om de overgedragen persoonsgegevens te **beschermen** tegen onvrijwillige of ongeoorloofde vernietiging, onvrijwillig verlies en ongeoorloofde toegang, wijziging of verspreiding.

3. Overgedragen persoonsgegevens worden **niet langer bewaard dan nodig is voor de doeleinden** waarvoor zij op grond van deze Overeenkomst worden verwerkt. De Partijen **houden onderling overleg over de noodzaak om** onjuiste, onvolledige of onbetrouwbare persoonsgegevens **te corrigeren** of over de wens of noodzaak om persoonsgegevens te wissen of het gebruik ervan te beperken.

4. De Partijen verzekeren dat er **passende veiligheidsmaatregelen** worden getroffen voor gegevens waaruit raciale of etnische afkomst, politieke opvattingen, godsdienstige of levensbeschouwelijke overtuiging, lidmaatschap van een vakbond, genetische persoonsgegevens, biometrische persoonsgegevens of persoonsgegevens over de gezondheid, het seksleven of de seksuele geaardheid van een persoon kunnen worden afgeleid.

5. Aan de veroordeelde persoon **kan informatie worden verstrekt** over de categorieën persoonsgegevens die worden overgedragen en over het doel van de overdracht van de persoonsgegevens.

6. De veroordeelde persoon heeft het **recht om een klacht in te dienen** indien hij/zij van mening is dat zijn/haar rechten met betrekking tot de verwerking van zijn/haar persoonsgegevens op grond van dit Overeenkomst zijn geschonden.

12. De Autoriteit herinnert eraan dat de EDPB richtsnoeren¹⁶ heeft vastgesteld met betrekking tot artikel 37 van de Richtlijn politie-justitie (zoals omgezet in artikel [68](#) van de WVG), die met name bedoeld zijn als leidraad voor de lidstaten bij onderhandelingen over nieuwe internationale instrumenten. De Autoriteit licht hieronder de belangrijkste lessen uit deze richtsnoeren toe en verwijst de aanvrager voor alles wat niet in dit advies is opgenomen naar deze richtsnoeren.

1. Vermeldingen in de memorie van toelichting bij de instemmingswet

13. De Autoriteit is, net als de EDPB, van oordeel dat in de memorie van toelichting bij de instemmingswet moet worden vermeld op welke elementen de Belgische onderhandelaars zich hebben gebaseerd om **de situatie betreffende de mensenrechten en de eerbiediging van de rechtsstaat** in het ontvangende land te **beoordelen**¹⁷.

2. Vermelding van de bepalingen die van toepassing zijn op persoonsgegevens

14. Artikel 7 van het ontwerp heeft specifiek betrekking op de bescherming van persoonsgegevens, wat door de Autoriteit positief wordt ontvangen.
15. De maatregelen waarover wordt gesproken in artikel 11 e.v. van het ontwerp (overlegging van documenten, registers, informatie, strafregisters, enzovoort) kunnen echter ook leiden tot de verwerking van persoonsgegevens.
16. De EDPB is van mening dat, wanneer bepalingen buiten het hoofdstuk "*Bescherming van persoonsgegevens*" toch betrekking hebben op de verwerking van "*informatie*", het essentieel is om duidelijk te vermelden of deze informatie persoonsgegevens kan bevatten. Indien dat het geval is, **moet een duidelijk onderscheid worden gemaakt met bepalingen die op andere soorten informatie dan persoonsgegevens betrekking hebben**¹⁸.
17. De Autoriteit is van oordeel dat de bepalingen van het ontwerp in het licht van het voorgaande moeten worden herzien.

¹⁶ Guidelines [01/2023](#), vastgesteld op 19 juni 2024.

¹⁷ *Ibidem*, punt 44.

¹⁸ *Ibidem*, punt 49.

3. Doeltreffendheid van de gegevensbescherming

18. De goedkeuring van een wet inzake gegevensbescherming door het derde land vormt een essentieel element, maar moet gepaard gaan met een analyse van de **doeltreffendheid van de implementatie ervan**¹⁹. Een dergelijke analyse moet ook aantonen dat de uitzonderingen waarop de rechtshandavingsinstanties een beroep kunnen doen, beperkt blijven tot wat evenredig en noodzakelijk is²⁰.
19. De Autoriteit is dan ook van oordeel dat in de memorie van toelichting bij de instemmingswet melding moet worden gemaakt van de geraadpleegde verslagen en dat de noodzaak en de evenredigheid van elke uitzondering waarop de bevoegde autoriteiten een beroep kunnen doen, moeten worden gemotiveerd.

4. Aandachtspunten bij de herformulering van de bepalingen inzake gegevensbescherming

20. De begrippen moeten door de partijen op gelijke wijze worden geïnterpreteerd, zodat zij niet kunnen worden **uitgelegd** op een manier die niet in overeenstemming is met de algemene beginselen en waarborgen die in de Europese Unie²¹ gelden voor wederzijdse rechtshulp in strafzaken. In dit verband is de Autoriteit van oordeel dat artikel 7 in ontwerp ernstige tekortkomingen vertoont, met name wat betreft de doeleinden van de gegevensverwerkingen (7.1.), de "passende" maatregelen voor gegevensbescherming en de "passende" veiligheidsmaatregelen (7.2. en 7.4.), de "noodzakelijke" bewaartermijn (7.3.), de voorwaarde voor overleg over de noodzaak van correctie (7.3.), de "mogelijkheid" om informatie te ontvangen (7.5.) en het "recht" om een klacht in te dienen (7.6.).
21. Een goede praktijk is om de bepalingen met betrekking tot met name de specifieke maatregelen voor gegevensbescherming, de categorieën van betrokkenen, de categorieën van gegevens, de communicatiekanalen en de spoedprocedures te **specificeren** in een **bijlage** die integraal deel uitmaakt van de overeenkomst²².

¹⁹ Zie bijvoorbeeld de analyse van het platform Civikos, pp. 28 e.v. (https://civikos.net/wp-content/uploads/2023/12/Raport-NED-eng_compressed.pdf).

²⁰ *Ibidem*, punt 45; er zij opgemerkt dat de AIP van Kosovo en de Kosovaarse politie een Memorandum of Understanding hebben ondertekend (zie <https://aip.rks-gov.net/en/the-information-and-privacy-agency-signed-a-memorandum-of-understanding-on-support-and-cooperation-with-the-kosovo-police/>).

²¹ *Ibidem*, punten 46, 53 en 54; zie over deze kwestie ook de Aanbevelingen [01/2021](#) van de EDPB over de adequaatheidsreferentie in het kader van de richtlijn gegevensbescherming bij rechtshandhaving, vastgesteld op 2 februari 2021.

²² *Ibidem*, punt 50.

22. Voorts dient uitdrukkelijk te worden vermeld dat de autoriteiten van de partijen die betrokken zijn bij de verwerkingen van persoonsgegevens waarop het Verdrag betrekking heeft (dus niet alleen de aangewezen centrale autoriteit), **uitsluitend bevoegde autoriteiten** zijn voor de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid, zoals bedoeld in artikel 1.1. van de Richtlijn politie-justitie²³.
23. **Verwijzingen naar andere normatieve kaders**, zowel nationale (zoals die in artikel 5.1. van het ontwerp) als internationale, mogen geen algemene verwijzingen zijn, maar moeten daarentegen specifieke bepalingen aanduiden die concrete waarborgen bieden, en dit enkel op voorwaarde dat uit een analyse van de wetgeving van het derde land blijkt dat het door de Richtlijn politie-justitie vereiste beschermingsniveau niet wordt afgezwakt²⁴.
24. Bovendien moeten de **bepalingen van het Verdrag**²⁵ (1) het toepassingsgebied ervan en de betrokken categorieën van gegevens vaststellen, (2) de verdere verwerking van gegevens aan voorwaarden onderwerpen, (3) de verplichting tot eerbiediging van het juistheidsbeginsel aan concrete verplichtingen koppelen, (4) een maximale bewaartermijn voor gegevens vastleggen, (5) beveiligingsmaatregelen voor gegevens opleggen, (6) een vertrouwelijkheidsplicht opleggen aan alle medewerkers die persoonsgegevens verwerken en specifieke verplichtingen voorschrijven in geval van een *data breach*, (7) de autoriteiten aanwijzen bij wie betrokkenen hun rechten kunnen uitoefenen, (8) de afwijkingen van de rechten van betrokkenen beperken, (9) bepalen dat de voorwaarden waaronder de overeenkomst de verwerking van doorgegeven gegevens regelt ook na beëindiging van de overeenkomst van toepassing blijven op die gegevens, en een informatieplicht opleggen in geval van wetswijzigingen die de overeenkomst aanzienlijk kunnen beïnvloeden.

4.1. Vaststelling van het toepassingsgebied van het Verdrag en van de betrokken categorieën van gegevens

25. Het toepassingsgebied van het Verdrag kan worden vastgesteld aan de hand van een lijst van strafbare feiten of van criteria die verband houden met de strafmaat.

²³ *Ibidem*, punten 52 en 59, iii; de lijst van bevoegde autoriteiten voor elk van de partijen kan in een bijlage of een latere verklaring worden opgenomen.

²⁴ *Ibidem*, punt 55.

²⁵ *Ibidem*, punt 59.

26. Wat de vaststelling van de categorieën van gegevens betreft, moeten in de eerste plaats de persoonsgegevens van het personeel van de bevoegde autoriteiten worden opgenomen (waarvan de verwerking noodzakelijk en evenredig is)²⁶.
27. Wat gegevens over strafbare feiten betreft (met inbegrip van gegevens uit strafregisters), dient vanwege het gevoelige karakter ervan te worden verwezen naar de gegevens die kunnen worden doorgegeven, en niet alleen naar de categorieën waartoe zij behoren. Bovendien moet worden verduidelijkt dat deze gegevens alleen mogen worden verwerkt voor zover dat noodzakelijk is, en moet uitdrukkelijk worden voorzien in extra waarborgen.
28. Tot slot is de Autoriteit van oordeel dat elke vorm van profilering van de betrokkene, op basis van een verwerking van gegevens die behoren tot bijzondere categorieën van gegevens en die tot discriminatie kunnen leiden, moet worden uitgesloten.

4.2. Verdere verwerking onderwerpen aan voorwaarden

29. Artikel 7.1. van het ontwerp onderwerpt de verdere verwerking van gegevens aan de voorafgaande toestemming van de partij die de gegevens doorgeeft.
30. De Autoriteit is echter van oordeel dat het wenselijk zou zijn om nog een stap verder te gaan, door – naast de voorafgaande schriftelijke toestemming van de partij aan wie de doorgifte van gegevens wordt gevraagd – ook een gemotiveerd verzoek van de verzoekende partij te eisen.
31. Bovendien is de Autoriteit van oordeel dat, tenzij de verdere verwerking van doorgegeven gegevens zonder meer wordt verboden, artikel 7.1. beter zou worden geherformuleerd door te verduidelijken dat een dergelijke verdere verwerking (met inbegrip van de mededeling aan andere autoriteiten van de ontvangende partij²⁷) alleen mogelijk is voor een doeleinde dat verenigbaar is met het doeleinde van de doorgifte en dat eveneens onder het toepassingsgebied van de Richtlijn politie-justitie valt (behalve in dringende gevallen om een ernstig en onmiddellijk gevaar voor de openbare veiligheid te voorkomen).

²⁶ Bijvoorbeeld hun identificatie- en/of contactgegevens.

²⁷ Dergelijke toegang moet in principe worden verboden, tenzij uitdrukkelijk toestemming wordt gegeven (in voorkomend geval met aanvullende voorwaarden naast die welke in het Verdrag zijn opgenomen) binnen een nader te bepalen termijn na de mededeling van schriftelijke informatie waarin de bevoegde ontvangende autoriteit (die eveneens onder de Richtlijn politie-justitie valt) wordt geïdentificeerd en de redenen voor het verzoek tot toegang en de betrokken categorieën van gegevens worden vermeld.

32. Indien van toepassing, moet tevens worden gepreciseerd dat "*de persoonsgegevens die worden verwerkt ter zake dienend en toereikend moeten zijn en beperkt moeten blijven tot wat noodzakelijk is voor het doeleinde van zowel de doorgifte als de verdere verwerking*".

4.3. Juistheidsbeginsel

33. Artikel 7.2. van het ontwerp bepaalt dat de partijen de juistheid van de doorgegeven gegevens moeten waarborgen.
34. In dit verband is de Autoriteit (net als de EDPB) van oordeel dat de verplichting tot eerbiediging van het juistheidsbeginsel moet worden gekoppeld aan concrete verplichtingen, zoals de verplichting tot kennisgeving en rectificatie of zelfs wissing.

4.4. Maximale bewaartermijn

35. Artikel 7.3. van het ontwerp bepaalt het volgende: "*Overgedragen persoonsgegevens worden **niet langer bewaard dan nodig is voor de doeleinden** waarvoor zij op grond van deze Overeenkomst worden verwerkt.*" Deze formulering is niet voldoende nauwkeurig om een betrokkene in staat te stellen te beoordelen of de gegevens nog steeds rechtmatig kunnen worden verwerkt.
36. Daarom moet deze bepaling worden geherformuleerd, waarbij – per categorie van gegevens en per doeleinde – de maximale bewaartermijn moet worden aangegeven, evenals het moment waarop die termijn begint te lopen.
37. Een goede praktijk bestaat erin om toegang tot de gegevens te beperken naarmate de bewaartermijn vordert (met andere woorden, de eerste X jaar een ruime toegang mogelijk maken, gevolgd door een beperkte toegang voor een bepaalde categorie medewerkers gedurende de daaropvolgende X jaar, en ten slotte een beperkte toegang, uitsluitend voor archiveringsdoeleinden, gedurende de laatste jaren van de bewaartermijn). Uiteraard moeten het noodzakelijke en evenredige karakter van deze bewaartermijnen en de bijbehorende toegang naar behoren worden gemotiveerd in de memorie van toelichting bij het ontwerp van instemmingswet.

4.5. Beveiligingsmaatregelen

38. Artikel 7.2. van het ontwerp verwijst naar "*passende maatregelen*" om de "*overgedragen*" gegevens te beschermen.

39. Zoals hierboven vermeld, is de Autoriteit van oordeel dat er concrete maatregelen moeten worden genoemd, zoals versleuteling, toegangscontrole op basis van het "*need-to-know*"-beginsel, regelmatige controle van logboeken, enzovoort.
40. Bovendien moet worden gepreciseerd dat deze maatregelen zowel moeten worden toegepast op de doorgifte van gegevens als op de verwerking ervan door de ontvanger.
41. De Autoriteit merkt overigens op dat artikel 2.4. van het ontwerp voorziet in de verzending van communicatie "*langs **elektronische weg** of via elk ander middel dat schriftelijk bewijs levert (...)*".
42. In dit verband is de Autoriteit van oordeel dat het verstrekken van gevoelige persoonsgegevens via e-mail in principe verboden moet zijn²⁸. In het onderhavige geval is er echter sprake van dergelijke gegevens, aangezien het met name gaat om gegevens over strafbare feiten zoals bedoeld in artikel 10 van de AVG.
43. Bovendien zal elektronische communicatie, tenzij gebruik wordt gemaakt van een (beveiligde) e-maildienst die toebehoort aan de verwerkingsverantwoordelijke zelf (en waarbij er dus geen sprake is van uitbesteding of gezamenlijke verwerkingsverantwoordelijkheid), zeer waarschijnlijk een doorgifte van persoonsgegevens naar een derde land en naar een andere verwerkingsverantwoordelijke dan een bevoegde autoriteit als bedoeld in het internationaal instrument in ontwerp met zich meebrengen²⁹. Daarom moeten er procedures en een communicatiekanaal worden ingevoerd die een beveiligingsniveau bieden dat past bij de aard van de doorgegeven gegevens.
44. In dit geval vereisen gegevens over strafbare feiten een hoog niveau van vertrouwelijkheid. Naast de algemene maatregelen zoals opgesomd in de normen inzake informatiebeveiliging (bijvoorbeeld NIST CSF, ISO 27001, 27002, 27701), kunnen met name – om een correct niveau van vertrouwelijkheid bij elektronische communicatie te bereiken – maatregelen worden getroffen met betrekking tot zowel het transmissiekanaal als het bericht (en de eventuele bijlagen) zelf, bijvoorbeeld door middel van (niet exhaustief):

²⁸ Zie in dit verband het advies van de Autoriteit nr. 223/2021 van 3 december 2021 over een ontwerpbesluit tot wijziging van het Besluit van het Verenigde College van COCOM van 10 maart 2016 houdende uitvoering van de ordonnantie van 21 juni 2012 betreffende de promotie van de gezondheid bij de sportbeoefening, het dopingverbod en de preventie ervan, overweging nr. 17, en het advies van de Autoriteit nr. 14/2022 van 21 januari 2022 over een ontwerpbesluit van de Waalse regering tot vaststelling van de samenstelling en de werking van het Waals Comité voor de bescherming van proefdieren (vrije vertaling; advies enkel in het Frans beschikbaar), overwegingen nrs. 21 tot en met 22.

²⁹ Zie hierover de adviezen 15/2015 (overwegingen 18 en 19) en 04/2017 van de CBPL, de voorganger van de Autoriteit.

- het gebruik van een online uitwisselingsplatform met veiligheidsnormen overeenkomstig de stand van de techniek. Op het internet wordt het gebruik van het TLS-protocol in een versie gelijk aan of hoger dan versie 1.2 beschouwd als een goede praktijk;
- het gebruik van een encryptiesoftware die de informatie onbegrijpelijk maakt voor iedereen die niet over de nodige informatie beschikt voor de decryptie (de sleutel), zoals de gratis compressietool "7-zip" waarbij de encryptiestandaard AES-256 wordt gebruikt. Hierbij geldt dat voor het verzenden van het versleutelde bericht en de overeenkomstige decoderingssleutel twee verschillende communicatiekanalen moeten worden gebruikt (bijvoorbeeld e-mail en vervolgens een applicatie);
- het gebruik van een hashingtechniek om na te gaan of de informatie tijdens de overdracht niet is gewijzigd. Net als bij versleuteling moet ervoor worden gezorgd dat alleen erkende en veilige algoritmen worden gebruikt (bijvoorbeeld SHA-512 en SHA-3). De hashfunctie moet worden toegepast op de platte tekst en aan deze platte tekst worden toegevoegd vóór de versleuteling (en niet op de versleutelde tekst).

45. Naast deze maatregelen is het ook raadzaam om voor elk systeem dat toegang geeft tot gevoelige gegevens (waaronder dus ook gegevens over strafbare feiten):

- het gebruik van authenticatie met minstens twee factoren verplicht te stellen (authenticatie bij het platform door een gebruikersnaam en een wachtwoord is onvoldoende);
- een strikt wachtwoordbeleid op te leggen (een willekeurig wachtwoord bestaande uit letters met een lengte van ten minste 17 tekens of een willekeurig wachtwoord bestaande uit alfanumerieke tekens (a-z, A-Z, 0-9, ...) met ten minste 14 tekens);
- van eventuele verwerkers en verdere verwerkers te eisen dat zij aan dezelfde veiligheidseisen voldoen.

46. Zoals hierboven aangegeven, kunnen deze elementen echter in een bijlage bij het Verdrag worden opgenomen.

47. De Autoriteit beveelt overigens aan om het bijhouden van een register van schriftelijke informatie-uitwisselingen³⁰ en de periodieke publicatie van (geanonimiseerde) statistieken verplicht te stellen.

4.6. Vertrouwelijkheidsplicht en maatregelen in geval van een data breach

48. Artikel 6.1. van het ontwerp verplicht de partij die wordt verzocht om gegevens over te dragen, om de vertrouwelijkheid van de feiten en de inhoud van het ontvangen verzoek tot gegevensoverdracht te waarborgen "overeenkomstig haar nationale wetgeving".

³⁰ In het bijzonder machtigingsaanvragen, verleende machtigingen, kennisgevingen, enzovoort.

49. Naast de (hierboven genoemde) problematiek van de algemene verwijzing naar een nationale norm, is de Autoriteit van oordeel dat het wenselijker zou zijn om te bepalen dat **het aan de ontvangende autoriteit is om het niveau van vertrouwelijkheid** (en dus van toegang) **te waarborgen dat door de overdragende autoriteit aan de informatie is toegekend**. De gedetailleerde regels kunnen ook in een bijlage worden vastgelegd, bijvoorbeeld indien de partijen overeenkomen om de door Interpol gehanteerde niveaus van vertrouwelijkheid toe te passen³¹.
50. De Autoriteit merkt overigens op dat aan de ontvangende partij geen specifieke verplichtingen worden opgelegd in geval van een **gegevenslek**. De Autoriteit is van oordeel dat het ontwerp op dit punt moet worden aangepast.

4.7. Toezichthoudende autoriteit

51. Artikel 7.6. van het ontwerp bepaalt het volgende: "*De veroordeelde persoon heeft het recht om een klacht in te dienen indien hij/zij van mening is dat zijn/haar rechten met betrekking tot de verwerking van zijn/haar persoonsgegevens op grond van dit Overeenkomst zijn geschonden.*"
52. De keuze voor deze formulering is waarschijnlijk te verklaren door het ontbreken van een wettelijke aanwijzing binnen de Belgische rechtsorde van een autoriteit die bevoegd is voor het toezicht op de verwerking van gegevens door de rechtbanken in het kader van de uitvoering van hun gerechtelijke taken. Desalniettemin is het nodig te **preciseren welke autoriteit** – onafhankelijk en uitgerust met de nodige middelen om haar taken uit te voeren – bevoegd is om dergelijke klachten te ontvangen³².
53. De keuze voor deze formulering kan echter ook wijzen op de wens van de partijen om te **voorzien in** administratieve en gerechtelijke **rechtsmiddelen**. In dit verband benadrukt de Autoriteit dat ervoor moet worden gezorgd dat deze rechtsmiddelen **doeltreffend** zijn en dat zij het als zodanig mogelijk maken voor alle betrokken personen (met inbegrip van personen die het grondgebied hebben verlaten, gevangen zitten, de nationale taal niet beheersen of niet over financiële middelen of specifieke juridische kennis beschikken) om toegang te krijgen tot deze rechtsmiddelen en, in voorkomend geval, een schadevergoeding te krijgen voor de geleden schade.
54. Het is een goede praktijk om te voorzien in een **uitwisseling van informatie** (met inbegrip van statistieken) tussen de partijen over de uitoefening van deze rechtsmiddelen.

³¹ Zie artikel [112](#), p. 41; ook al is Kosovo geen lid van Interpol.

³² Of op zijn minst te eisen dat deze informatie openbaar en gemakkelijk toegankelijk is.

55. De Autoriteit is ook van oordeel dat ervoor moet worden gezorgd dat een partij zich niet kan **onttrekken aan haar verantwoordelijkheid** jegens de betrokken personen door zich te beroepen op het feit dat een andere partij onjuiste of verouderde gegevens heeft verstrekt.

4.8. Afwijkingen van de rechten van de betrokkene

56. Wat de rechten van betrokkenen betreft, vermeldt artikel 7.5. van het ontwerp de "*mogelijkheid*" om informatie te ontvangen over de categorieën van gegevens die worden doorgegeven en over de doeleinden van de doorgifte. Door te verwijzen naar een "mogelijkheid" in plaats van een "recht" kan deze bepaling worden geïnterpreteerd als een bepaling die de bevoegde autoriteit een discretionaire beoordelingsbevoegdheid verleent. Bovendien stelt deze formulering (doordat zij geen duidelijkheid schept over de verplichtingen van de verwerkingsverantwoordelijke bij een verzoek van een betrokkene om zijn rechten uit te oefenen) de betrokkene niet in staat te beoordelen of een eventuele weigering noodzakelijk en evenredig is.
57. Bijgevolg is de Autoriteit van oordeel dat deze formulering moet worden herzien door duidelijk aan te geven welke autoriteiten verplicht zijn te reageren op een verzoek tot toegang en in welke **specifieke omstandigheden** zij een dergelijk verzoek mogen weigeren.
58. Concreet is de Autoriteit van oordeel dat deze **afwijkingen uitdrukkelijk beperkt moeten blijven** tot de in artikel 16.4 van de Richtlijn politie-justitie genoemde redenen. In voorkomend geval zou kunnen worden overwogen om een **beperking op de doorgifte** van persoonsgegevens op te leggen (overeenkomstig artikel 16 van de Richtlijn politie-justitie) zolang de juistheid ervan wordt onderzocht.
59. Er zij op gewezen dat het een goede praktijk is om de opstelling en de publicatie van **statistieken** over verzoeken van betrokkenen tot uitoefening van hun rechten verplicht te stellen.

4.9. Handhaving van de werking van het Verdrag en informatieplicht

60. De Autoriteit beveelt aan te bepalen dat de voorwaarden die in de overeenkomst worden gesteld aan de verwerking van doorgegeven gegevens, van toepassing blijven op deze gegevens, ook na beëindiging van de overeenkomst. In dit verband is het een goede praktijk om te **voorzien in een verkorte bewaartermijn in geval van beëindiging** en om **elke verdere doorgifte** van de gegevens te **verbieden**.

61. Ten slotte beveelt de Autoriteit aan een informatieplicht jegens de andere partij op te leggen in geval van **wetswijzigingen** die de overeenkomst aanzienlijk kunnen beïnvloeden³³.

5. Gebruik van videoconferentie

62. Artikel 17 van het ontwerp regelt de mogelijkheid om een verhoor per videoconferentie te houden, *"voor zover mogelijk en in overeenstemming met de fundamentele beginselen van het recht van de Aangezochte Partij"*.
63. De Autoriteit herinnert eraan dat het noodzakelijke en evenredige karakter van de maatregel in de memorie van toelichting bij de instemmingswet moet worden gemotiveerd. Indien bij die gelegenheid blijkt dat artikel 17 van het ontwerp moet worden aangepast, roept de Autoriteit de aanvrager op om kennis te nemen van de opmerkingen in advies 63/2023³⁴ van de Autoriteit en advies 3/2023³⁵ van het Federaal Instituut voor de bescherming en de bevordering van de Rechten van de Mens, met het oog op de herformulering van deze bepaling.

OM DEZE REDENEN,

De Autoriteit

is ingenomen met het feit dat zij voorafgaand aan de ondertekening van het ontwerp van Verdrag door de partijen is geraadpleegd;

is van oordeel dat het ontwerp grondig moet worden herzien in het licht van de hierboven geformuleerde opmerkingen;

herinnert eraan dat dit advies de aanvrager niet ontslaat van de verplichting om het ontwerp van instemmingswet, vergezeld van het aangepaste ontwerp van Verdrag, ter advies voor te leggen aan de Autoriteit;

vestigt de aandacht van de aanvrager op het bestaan van de richtsnoeren 01/2023 van de EDPB met betrekking tot artikel 37 van de Richtlijn politie-justitie.

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

³³ *Op. cit.*, punt 60, vii.

³⁴ Uitgebracht op 9 maart 2023.

³⁵ Uitgebracht op 31 januari 2023.