Advies nr. 57/2017 van 11 oktober 2017

Betreft: Advies uit eigen beweging betreffende het wetsontwerp tot wijziging van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen en van de wet van 12 januari 2007 betreffende de opvang van asielzoekers en van bepaalde andere categorieën van vreemdelingen (CO-A-2017-047)

De Commissie voor de bescherming van de persoonlijke levenssfeer;

Gelet op de wet van 8 december 1992 *tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens* (hierna WVP), inzonderheid artikel 29;

Gelet op de aanvullende informatie van de Commissaris-generaal voor de Vluchtelingen en Staatlozen, ontvangen op 29 augustus en 5 september 2017;

Gelet op het verslag van de heer Willem Debeuckelaere;

Brengt op 11 oktober 2017 het volgend advies uit:

VOORAFGAANDE OPMERKINGEN

De Commissie vestigt er de aandacht op dat er recent nieuwe Europese regelgeving inzake de bescherming persoonsgegevens werd uitgevaardigd: de algemene Verordening betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en de Richtlijn voor Politie en Justitie. Deze teksten verschenen in het Europese Publicatieblad van 4 mei 2016[1].

De verordening, meestal AVG (Algemene Verordening Gegevensbescherming) genaamd, is van kracht geworden twintig dagen na publicatie, nl. op 24 mei 2016 en wordt, twee jaar later, automatisch van toepassing: 25 mei 2018. De richtlijn voor politie en justitie moet via nationale wetgeving omgezet worden tegen uiterlijk 6 mei 2018.

Voor de Verordening betekent dit dat vanaf 24 mei 2016, en gedurende de termijn van twee jaar voor de tenuitvoerlegging, op de lidstaten enerzijds een positieve verplichting rust om alle nodige uitvoeringsbepalingen te nemen en anderzijds ook een negatieve verplichting, de zogenaamde “onthoudingsplicht”. Laatstgenoemde plicht houdt in dat er geen nationale wetgeving mag worden uitgevaardigd die het door de Verordening beoogde resultaat ernstig in gevaar zou brengen. Ook voor de Richtlijn gelden gelijkaardige principes.

Het verdient dan ook aanbeveling om desgevallend nu reeds op deze teksten te anticiperen. En het is in de eerste plaats aan de adviesaanvrager(s) om hier rekening mee te houden in zijn (hun) voorstellen of ontwerpen. De Commissie heeft in onderhavig advies, in de mate van het mogelijke en onder voorbehoud van mogelijke bijkomende toekomstige standpunten, alvast gewaakt over de hoger geschetste negatieve verplichting.

---

[1] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming)

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

http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=OJ:L:2016:119:TOC

http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=OJ%3AL%3A2016%3A119%3ATOC)

I. CONTEXT VAN DE ADVIESAANVRAAG

1. De Commissie wenst advies uit te brengen over het *wetsontwerp tot wijziging van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen en de wet van 12 januari 2007 betreffende de opvang van asielzoekers en van bepaalde andere categorieën van vreemdelingen*, hierna het voorontwerp.

2. Met het wetsontwerp worden verschillende Europese richtlijnen in de Belgische rechtsorde omgezet, waaronder, van belang voor onderhavig advies, de Richtlijn 2013/32/EU van 26 juni 2013 (Richtlijn 2013/32/EU) [1] De omzetting van deze laatste heeft gevolgen voor de wijze van het onderzoek in het kader van de asielprocedure. De Richtlijn 2013/32/EU verwijst naar de toepassing van de Richtlijn 95/46/EG van 24 oktober 1995 betreffende de verwerking van persoonsgegevens.[2]

3. Het advies heeft specifiek betrekking op artikel 10 van het wetsontwerp, hetwelk het huidige artikel 48/6 van de wet van 15 december 1980 *betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen* (de Vreemdelingenwet) zal vervangen. Zoals verder wordt aangetoond, heeft deze bepaling betrekking op de verwerking van persoonsgegevens van asielzoekers, met name hun identiteit en talrijke gegevens die het privéleven raken. Bijgevolg is de WVP van toepassing.

4. De Commissie stelt vast dat het wetsontwerp op 10 augustus 2017 door de Commissie voor Binnenlandse Zaken, de Algemene Zaken en het Openbaar Ambt is aangenomen. De Commissie herinnert aan artikel 29, § 1, WVP volgens hetwelk de Commissie op onder meer verzoek van de Regering of de Wetgevende Kamers advies uitbrengt *omtrent iedere aangelegenheid die betrekking heeft op de grondbeginselen van de persoonlijke levenssfeer, in het kader van deze wet en van wetten die bepalingen bevatten inzake de bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens*. De Commissie ontving geen verzoek vanwege de staatssecretaris voor Asiel en Migratie over het wetsontwerp.

5. Hoewel de WVP de raadpleging van de Commissie niet oplegt, vestigt de Commissie er louter volledigheidshalve de aandacht op dat:

- artikel 28, lid 2 van de Richtlijn 95/46/EG raadpleging van de Commissie vereist;

---

[1] Richtlijn 2013/32/EU van 26 juni 2013 van het Europees Parlement en de Raad *betreffende gemeenschappelijke procedures voor de toekenning en intrekking van de internationale bescherming (herziening)*.

[2] Richtlijn 95/46/EG van 24 oktober 1995 van het Europees Parlement en de Raad *betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens*.

- sinds de inwerkingtreding van de AVG op 24 mei 2016 advies *moet* gevraagd worden omtrent verwerkingen van persoonsgegevens die waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van natuurlijke personen.[3]

De uit de hoger voorgestelde wetswijziging voortspruitende verwerking van persoonsgegevens (controle van de smartphone van asielzoekers, diens participatie op sociale netwerken of andere drager van digitale informatie) moet als verwerking met een waarschijnlijk hoog risico gekwalificeerd worden.[4]

II. ONDERZOEK VAN HET WETSONTWERP BEPERKT TOT ARTIKEL 10, § 1, VIERDE LID

A. Algemeen beschouwingen

6. Artikel 10 van het aangenomen wetsontwerp behoudt de principiële medewerkingsplicht van de asielzoeker. Dit houdt in dat de asielzoeker tijdens de asielprocedure zijn of haar volle medewerking moet verlenen aan het onderzoek. Aldus rust op de asielzoeker de plicht om tijdens het onderzoek ten overstaan van de Commissaris-generaal voor de Vluchtelingen en Staatlozen (CGVS) de nodige feiten en relevante elementen aan te brengen op basis waarvan de CGVS een beslissing kan nemen over het verzoek om internationale bescherming.

7. Deze feiten en elementen hebben onder meer betrekking op de leeftijd, de achtergrond, identiteit, geslacht, nationaliteit en verblijfplaatsen van de verzoeker. De medewerkingsplicht van de asielzoeker bestaat erin dat deze de nodige documenten en documentatie aan de medewerkers van de CGVS overlegt zodat de asielaanvraag correct kan beoordeeld worden (zie artikel 48/6 Vreemdelingenwet).

8. Met betrekking tot deze medewerkingsplicht voert artikel 10, § 1, vierde lid, van het wetsontwerp een belangrijke nieuwigheid in die het voorwerp uitmaakt van onderhavig advies: "*Indien de met het onderzoek belaste instanties goede redenen hebben om aan te nemen dat de verzoeker informatie, stukken, documenten of andere elementen achterhoudt die essentieel zijn voor de correcte beoordeling van het verzoek, kunnen zij de verzoeker uitnodigen om deze elementen onverwijld voor te leggen, wat ook hun drager is. De weigering van de verzoeker om deze elementen voor te leggen zonder bevredigende verklaring kan een aanwijzing zijn van zijn weigering om te voldoen aan zijn medewerkingsplicht zoals bedoeld in het eerste lid*."

[3] Hoewel de AVG pas kan afgedwongen worden vanaf 25 mei 2018.

[4] Zie de artikelen 57, lid 1, 36, lid 2 en 35 GDPR/AVG.

9. Uit artikel 10 van het wetsontwerp volgt dat deze medewerkingsplicht voortaan ook betrekking heeft op het aanleveren van bewijs door het verkrijgen van toegang tot afgeschermde informatie op sociale netwerksites, de smartphone, USB-stick, CD-rom, geheugenkaart, enz. die de asielzoeker bij zich draagt. Dit gebeurt volgens de memorie van toelichting op basis van de toestemming van de asielzoeker.[5]

10. Verder wordt in de memorie van toelichting geponeerd dat de controle van de informaticasystemen en afgeschermde sociale netwerksites in overeenstemming is met de WVP.[6]

B. Ten aanzien van de controle van de informatiesystemen van de asielzoeker

11. Volgens de aanvullende informatie verstrekt door de CGVS kan de toegang tot de digitale omgeving van de asielzoeker slechts worden gevraagd wanneer dat noodzakelijk is om de CGVS in staat te stellen het verzoek om, en dus de nood aan, internationale bescherming te boordelen. De toegang tot de digitale omgeving op de smartphone en/of afgeschermde sociale netwerksites van de asielzoeker om het bewijs te leveren van zijn of haar identiteit, afkomst en/of gevaar voor vervolging en bescherming tegen oorlogsgeweld kan dus niet op systematische wijze worden uitgevoerd.

12. Bovendien heeft de (medewerker van de) CGVS slechts toegang tot het private gedeelte van digitale informatie van de asielzoeker indien deze laatste daarmee *instemt*. Volgens de staatssecretaris van Asiel en Migratie was dit reeds een gangbare praktijk.[7] Dit wordt bevestigd door de aanvullende informatie van de CGVS: "*In de praktijk wordt de vraag tot toegang tot sociale media (bijvoorbeeld het privé-gedeelte van facebook) dus door de medewerkers van het CGVS gevraagd wanneer er indicaties zijn dat de betrokkene bepaalde informatie -noodzakelijk voor de beoordeling- achterhoudt. Dit gebeurt bijgevolg in een beperkt aantal gevallen. De informatie op andere informatiedragers (gsm, laptop, …) wordt enkel gelezen wanneer de betrokkene zelf deze informatie voorlegt*."

13. De Commissie stelt zich vragen bij de uitbreiding van deze opsporingsmaatregel naar de administratieve overheid. Zonder analogie te willen maken met het voorliggend wetsontwerp, verwijst de Commissie naar de bevoegdheden van, bijvoorbeeld, de politie inzake de controle van een in beslag genomen smartphone[8] of de bevoegdheid van sociale inspecteurs om zich toegang te verschaffen tot

---

[5] Memorie van toelichting bij het wetsontwerp (MvT), p. 34. Verslag bij het wetsontwerp namens de Commissie voor de Binnenlandse Zaken, de Algemene Zaken en het Openbaar Ambt, uitgebracht door mevrouw Monica De Coninck, DOC 54-2548/02, p.18.

[6] Mvt, p. 36: "*Dit lid is in overeenstemming met de wet van 8 december 1992 voor de bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens*"

[7] Verslag bij het wetsontwerp namens de Commissie voor de Binnenlandse Zaken, de Algemene Zaken en het Openbaar Ambt, uitgebracht door mevrouw Monica De Coninck, DOC 54-2548/02, p. 27.

[8] Art. 39bis Wetboek van Strafvordering (Sv).

"§ 1Onverminderd de specifieke bepalingen van dit artikel, zijn de regels van dit wetboek inzake inbeslagneming, met inbegrip van artikel 28sexies, van toepassing op het kopiëren, ontoegankelijk maken en verwijderen van in een informaticasysteem of een deel ervan opgeslagen gegevens.
§ 2. Tot de zoeking in een informaticasysteem of een deel ervan dat in beslag genomen is, kan beslist worden door een officier van gerechtelijke politie.
Onverminderd het eerste lid, kan de procureur des Konings een zoeking bevelen in een informaticasysteem of een deel ervan dat door hem in beslag kan worden genomen.
De zoekingen bedoeld in het eerste en het tweede lid kunnen zich enkel uitstrekken tot de gegevens die opgeslagen zijn op het informaticasysteem dat, respectievelijk, in beslag genomen is of in beslag kan worden genomen. Met het oog daarop wordt elke externe verbinding van dit informaticasysteem verhinderd, alvorens de zoeking wordt aangevat.
§ 3. De procureur des Konings kan de zoeking in een informaticasysteem of een deel ervan, aangevat op grond van paragraaf 2, uitbreiden naar een informaticasysteem of een deel ervan dat zich op een andere plaats bevindt dan daar waar de zoeking plaatsvindt:
- indien deze uitbreiding noodzakelijk is om de waarheid aan het licht te brengen ten aanzien van het misdrijf dat het voorwerp uitmaakt van de zoeking; en
- indien andere maatregelen disproportioneel zouden zijn, of indien er een risico bestaat dat zonder deze uitbreiding bewijselementen verloren gaan.
De uitbreiding van de zoeking in een informaticasysteem mag zich niet verder uitstrekken dan tot de informaticasystemen of de delen ervan waartoe de personen die gerechtigd zijn het onderzochte informaticasysteem te gebruiken, in het bijzonder toegang hebben.
Inzake de door uitbreiding van de zoeking in een informaticasysteem aangetroffen gegevens, die nuttig zijn voor dezelfde doeleinden als de inbeslagneming, wordt gehandeld zoals bepaald in paragraaf 6.
Wanneer blijkt dat deze gegevens zich niet op het grondgebied van het Rijk bevinden, worden ze enkel gekopieerd. In dat geval deelt de procureur des Konings dit onverwijld mee aan de Federale Overheidsdienst Justitie, dat de bevoegde overheid van de betrokken Staat hiervan op de hoogte brengt, indien deze redelijkerwijze kan worden bepaald.
In geval van uiterst dringende noodzakelijkheid kan de procureur des Konings de uitbreiding van de zoeking bedoeld in het eerste lid mondeling bevelen. Dit bevel wordt zo spoedig mogelijk schriftelijk bevestigd, met vermelding van de redenen van de uiterst dringende noodzakelijkheid.
§ 4. Enkel de onderzoeksrechter kan een andere zoeking bevelen in een informaticasysteem of een deel ervan dan de zoekingen voorzien in de paragrafen 2 en 3:
- indien deze zoeking noodzakelijk is om de waarheid aan het licht te brengen ten aanzien van het misdrijf dat het voorwerp uitmaakt van de zoeking; en
- indien andere maatregelen disproportioneel zouden zijn, of indien er een risico bestaat dat zonder deze zoeking bewijselementen verloren gaan.
In geval van uiterst dringende noodzakelijkheid kan de onderzoeksrechter de uitbreiding van de zoeking bedoeld in het eerste lid mondeling bevelen. Dit bevel wordt zo spoedig mogelijk schriftelijk bevestigd, met vermelding van de redenen van de uiterst dringende noodzakelijkheid.
§ 5. Teneinde de maatregelen bedoeld in dit artikel mogelijk te maken, kan de procureur des Konings of de onderzoeksrechter bevelen om, te allen tijde, ook zonder de toestemming van hetzij de eigenaar of zijn rechthebbende, hetzij de gebruiker:
- elke beveiliging van de betrokken informaticasystemen tijdelijk op te heffen, desgevallend met behulp van technische hulpmiddelen, valse signalen, valse sleutels of valse hoedanigheden;
- technische middelen in de betrokken informaticasystemen aan te brengen teneinde de door dat systeem opgeslagen, verwerkte of doorgestuurde gegevens te ontcijferen en te decoderen.
Evenwel kan enkel de onderzoeksrechter deze tijdelijke opheffing van de beveiliging of deze aanbrenging van technische middelen bevelen wanneer dit in het bijzonder noodzakelijk is voor de toepassing van paragraaf 3.
§ 6. Indien in de betrokken informaticasystemen opgeslagen gegevens aangetroffen worden die nuttig zijn voor dezelfde doeleinden als de inbeslagneming, maar de inbeslagneming van de drager daarvan evenwel niet wenselijk is, worden deze gegevens, evenals de gegevens noodzakelijk om deze te kunnen verstaan, gekopieerd op dragers, die toebehoren aan de overheid. In geval van dringendheid of om technische redenen, kan gebruik gemaakt worden van dragers, die ter beschikking staan van personen die gerechtigd zijn om het informaticasysteem te gebruiken. Bovendien worden passende technische middelen aangewend om de toegang tot deze gegevens in het informaticasysteem, evenals tot de kopieën daarvan die ter beschikking staan van personen die gerechtigd zijn om het informaticasysteem te gebruiken, te verhinderen en hun integriteit te waarborgen. Wanneer de in het eerste lid vermelde maatregel niet mogelijk is om technische redenen of wegens de omvang van de gegevens, wendt de procureur des Konings de passende technische middelen aan om de toegang tot deze gegevens in het informaticasysteem, evenals tot de kopieën daarvan die ter beschikking staan van personen die gerechtigd zijn om het informaticasysteem te gebruiken, te verhinderen en hun integriteit te waarborgen. Indien de gegevens het voorwerp van het misdrijf vormen of voortgekomen zijn uit het misdrijf en indien de gegevens strijdig zijn met de openbare orde of de goede zeden, of een gevaar opleveren voor de integriteit van informaticasystemen of gegevens die door middel daarvan worden opgeslagen, verwerkt of overgedragen, wendt de procureur des Konings alle passende technische middelen aan om deze gegevens ontoegankelijk te maken of, na hiervan kopie te hebben genomen, te verwijderen. Hij kan evenwel, behoudens in het geval bedoeld in het vierde lid, het verdere gebruik van het geheel of een deel van deze gegevens toestaan, wanneer dit geen gevaar voor de strafvordering oplevert. In geval van uiterst dringende noodzakelijkheid en wanneer het kennelijk gaat om een strafbaar feit bedoeld in de artikelen 137, § 3, 6°, 140bis of 383bis, § 1, van het Strafwetboek, kan de procureur des Konings mondeling bevelen dat alle passende technische middelen worden aangewend om de gegevens, die het voorwerp van het misdrijf vormen of voortgekomen zijn uit het misdrijf en die strijdig zijn met de openbare orde of de goede zeden, ontoegankelijk te maken. Dit bevel wordt zo spoedig mogelijk schriftelijk bevestigd, met vermelding van de redenen van de uiterst dringende noodzakelijkheid.
§ 7. Tenzij diens identiteit of woonplaats redelijkerwijze niet achterhaald kan worden, brengt de procureur des Konings of de onderzoeksrechter de verantwoordelijke van het informaticasysteem zo spoedig mogelijk op de hoogte van de zoeking in het

informatiesystemen met het oog op de controle van de naleving van de sociale wetgeving. In beide gevallen is het (uit)lezen van informaticasystemen slechts toegelaten in specifieke omstandigheden en omkleed met de nodige waarborgen. Deze strenge voorwaarden worden door de wetgever opgelegd omdat de informatie op een smartphone en afgeschermde sociale netwerksites een zeer uitgebreid en gedetailleerd beeld verschaft over (de kern van) het privéleven van de gebruiker, en veelal ook dat van derden. Daarmee geeft de wetgever te kennen dat het een verregaande inbreuk op het privéleven is tot dewelke men slechts in specifieke gevallen zijn toevlucht kan nemen, mits inachtneming van wettelijke waarborgen.

14. In tegenstelling tot de ambtenaren van de politie en de sociale inspectie, zijn de medewerkers van CGVS niet opgeleid om deze verregaande bevoegdheden uit te oefenen noch hebben zij taken die initieel thuishoren in (bijzondere) strafwetgeving. Indien de medewerker van de CGVS tijdens het onderzoek van de asielaanvraag op aanwijzingen van strafbare feiten zou stuiten, dan dient daarvan aangifte te worden gedaan aan de procureur des Konings overeenkomstig artikel 29 SV.

C. Met betrekking tot de toestemming van de asielzoeker

15. Uit artikel 10, § 1, vierde lid, van het wetsontwerp blijkt dat de medewerker van de CGVS slechts toegang tot de drager kan vragen wanneer er "*goede redenen*" zijn om aan te nemen dat de asielzoeker informatie, stukken, documenten of andere elementen "*achterhoudt*" die noodzakelijk zijn om het verzoek van de asielzoeker correct te kunnen beoordelen. Het gaat bijvoorbeeld om lacunes in de verklaringen, incoherenties of tegenstrijdigheden tussen de informatie die door de asielzoeker wordt verstrekt en andere beschikbare informatie.[9] De toegang tot de privécommunicatie van de asielzoeker is dus louter gebaseerd op de beoordelingsbevoegdheid van de CGVS.

16. De vaststelling van de medewerker van de CGVS dat de asielzoeker de nodige informatie achterhoudt, kan er toe leiden dat de asielzoeker wordt gevraagd om informatie die in een informaticasysteem dat hij bij zich draagt is opgeslagen, voorlegt. Zonder de toestemming van de asielzoeker kan de medewerker zich geen toegang verschaffen tot de opgeslagen gegevens op de drager. De Commissie maakt daarbij onderscheid tussen de situatie waarbij de asielzoeker de informatie uit eigen beweging zelf aan de medewerker van de CGVS voorlegt en deze waarbij de

---

informaticasysteem of van de uitbreiding ervan. Hij deelt hem in voorkomend geval een samenvatting mee van de gegevens die zijn gekopieerd, ontoegankelijk gemaakt of verwijderd.
§ 8. De procureur des Konings wendt de passende technische middelen aan om de integriteit en de vertrouwelijkheid van deze gegevens te waarborgen.
Gepaste technische middelen worden aangewend voor de bewaring hiervan op de griffie.
Hetzelfde geldt, wanneer gegevens die worden opgeslagen, verwerkt of overgedragen in een informaticasysteem, samen met hun drager in beslag worden genomen, overeenkomstig de vorige artikelen.

[9] MvT, p. 34-36.

asielzoeker wordt gevraagd om toegang te verschaffen tot de digitale informatiesystemen die hij bij zich draagt of privé-informatie op sociale netwerksites. Het is evident dat door artikel 10, § 1, vierde lid, alleen de laatste situatie viseert, aangezien het iedereen vrij staat om spontaan digitale informatie met een derde te delen.

17. In de WVP wordt "toestemming" omschreven als "*elke vrije, specifieke en op informatie berustende wilsuiting, waarmee de betrokkene of zijn wettelijke vertegenwoordiger aanvaardt dat persoonsgegevens betreffende de betrokkene worden verwerkt*"[10]. Vraag is of van de toestemming van de asielzoeker, zoals hiervoor omschreven, *de facto* sprake is. Er kan namelijk moeilijk worden aangenomen dat de asielzoeker in de gegeven omstandigheden zijn of haar toestemming "vrij" zal verstrekken[11]. In de eerste plaats bepaalt artikel 10, § 1, vierde lid van het ontwerp dat de CGVS "*de verzoeker uitnodigen om deze elementen onverwijld voor te leggen, wat ook hun drager is*". De betrokkene bevindt zich dus in een afhankelijk positie waarbij de vraag van de medewerker van het CGVC om toegang te krijgen tot de smartphone of de privé-informatie op de Facebookpagina van de asielzoeker in diens hoofde al snel als gebod of verplichting zal worden beschouwd. Deze perceptie in hoofde van de asielzoeker zal nog versterkt worden doordat de asielzoeker wordt medegedeeld dat bij gebrek aan "*bevredigende verklaring*" voor zijn weigering om toegang te verlenen tot deze digitale informatiesystemen, dit als een tekortkoming in de medewerkingsplicht wordt beschouwd.[12] En dit gebrek aan medewerking kan als een negatief element beschouwd worden bij de beoordeling van het verzoek om internationale bescherming.[13] Hieruit volgt dat de toestemming dus niet wordt losgekoppeld van de plicht tot medewerking in hoofde van de asielzoeker.

D. Met betrekking tot de toegang tot de informaticasystemen van de asielzoeker

18. Meer fundamenteel stelt de Commissie ernstige gebreken vast ten aanzien van de kwaliteit van artikel 10, § 1, vierde lid van het wetsontwerp. Wanneer de overheid door het verwerken van persoonsgegevens afbreuk doet aan de bescherming van de persoonlijke levenssfeer, moeten

---

[10] Art. 1, § 8 WVP. In het licht van de toekomstige toepassing van de GDPR vestigt de Commissie er de aandacht op de definitie van "toestemming" die niet precies gelijkluidend is met de definitie onder de WVP. Dat komt onder meer omdat in de verordening wordt rekening gehouden met de toestemming in een digitale omgeving. Art. 4, 11) GDPR omschrijft toestemming als "*elke vrije specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt*". Uit overweging 32 bij artikel 4, 11) GDPR blijkt dat de toestemming kan worden verstrekt door middel van een duidelijke actieve handeling met gebruik van elektronisch middelen. Uit deze actieve handeling, gebaseerd op duidelijke en specifieke informatie over het doel waarvoor de toestemming wordt gegeven en de gevolgen ervan, moet de weloverwogen en ondubbelzinnige toestemming van de betrokkene blijken.

[11] Art. 1, § 8 WVP: "*Onder "toestemming van de betrokkene" wordt elke vrije, specifieke en op informatie berustende wilsuiting verstaan, waarmee de betrokkene of zijn wettelijke vertegenwoordiger aanvaardt dat persoonsgegevens betreffende de betrokkene worden verwerkt"*.

[12] MvT, p. 34-36.

[13] Ibid.

waarborgen worden ingebouwd tegen arbitraire maatregelen en beslissingen. Dit is *in casu* niet het geval. Artikel 10 van het wetsontwerp geeft geen uitsluitsel over de volgende vragen:
- Op welke manier wordt de toegang tot de drager van digitale informatie verstrekt? Wordt de drager door de medewerker van de CGVS doorzocht naar relevante informatie of behoudt de asielaanvrager de macht over zijn drager zodat hij zelf de toegang tot een selectie van informatie kan verstrekken?
- Op welke manier wordt de verkregen digitale informatie opgeslagen?
- Wordt enkel de relevante informatie opgeslagen dan wel overgeschreven in een verslag, of alle informatie die door de medewerker van de CGVS wordt gelezen?
- Door wie wordt de verstrekte informatie vertaald en geïnterpreteerd?
- Op welke manier wordt de verstrekte digitale informatie beveiligd en de authenticiteit ervan gewaarborgd?

19. De Commissie stelt vast dat een afdoend wettelijk kader met betrekking tot de wijze waarop de toegang tot de digitale drager geschiedt enerzijds, en de rechten van de betrokkene anderzijds ontbreekt. Artikel 10, § 1, vierde lid, van het ontwerp bepaalt slechts dat wanneer de asielzoeker informatie, stukken, documenten of andere elementen achterhoudt die essentieel zijn om het verzoek om bescherming correct te beoordelen, de asielzoeker kan uitgenodigd worden om deze elementen "*onverwijld"* voor te leggen, los van de drager waarop de informatie is opgeslagen. Het tweede lid van paragraaf twee van artikel 10 van het wetsontwerp lijkt betrekking te kunnen hebben op de digitale informatie die door de CGVS wordt verkregen, doch is te vaag en in algemene bewoordingen gesteld gelet op de aard van de onderzoeksmaatregel.

OM DEZE REDENEN

Verstrekt de Commissie **ongunstig** advies.

De Wnd. Administrateur, De Voorzitter,

(get.) An Machtens (get.) Willem Debeuckelaere