



Advies nr. 84/2018 van 14 september 2018

Betreft: Wetsontwerp tot vaststelling van een kader voor de beveiliging van netwerk –en informatiesystemen van algemeen belang voor de openbare veiligheid (CO-A-2018-070)

De Gegevensbeschermingsautoriteit (hierna “de Autoriteit”);

Gelet op de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit, inzonderheid de artikelen 23 en 26;

Gelet op het verzoek om advies van Dhr. Michel, Eerste Minister, ontvangen op 20 juli 2018;

Gelet op het verslag van Dhr. F. De Smet;

Brengt op 14 september 2018 het volgend advies uit:

I. VOORWERP EN CONTEXT VAN DE ADVIESAANVRAAG

1. De Eerste Minister (hierna "de aanvrager") verzocht op 20 juli 2018 het advies van de Autoriteit over een wetsontwerp *tot vaststelling van een kader voor de beveiliging van netwerk –en informatiesystemen van algemeen belang voor de openbare veiligheid* (hierna "het Ontwerp").
2. Het Ontwerp beoogt de omzetting van de Europese Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 *houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk –en informatiesystemen in de Unie* (hierna "de Richtlijn"). De verplichtingen vervat in de richtlijn gelden voornamelijk voor entiteiten die, ingeval van een incident dat de beveiliging van hun netwerk –en informatiesystemen aantast, de verlening van essentiële diensten en van digitale diensten voor het behoud van kritieke maatschappelijke of economische activiteiten aanzienlijk kunnen verstoren¹. De richtlijn heeft met name tot doel ervoor te zorgen dat technische –en organisatorische beveiligingsmaatregelen worden genomen door de aanbieders van essentiële diensten en door digitale dienstverleners om incidenten te voorkomen of de impact ervan te beperken, teneinde de continuïteit van deze diensten te waarborgen. In dezelfde geest heeft de in de Richtlijn vervatte meldingsplicht van incidenten betrekking op de incidenten die een aanzienlijke impact hebben op de verleende diensten².
3. Verschillende autoriteiten worden belast met de uitvoering van de bepalingen in het Ontwerp. De Koning zal met name meerdere autoriteiten aanwijzen die de volgende rollen zullen opnemen³:
 - Nationale autoriteit, die belast is met de opvolging en coördinatie van de uitvoering van deze wet. Deze nationale autoriteit is ook het "Centraal Nationaal Contactpunt". Dit betreft een verbindingsfunctie – gecreëerd door de Richtlijn – die moet zorgen voor Europese samenwerking;
 - Nationaal Computer Security Incident Response Team (hierna het "NCSIRT"), dat belast is met de ontvangst en behandeling van meldingen van incidenten door aanbieders van essentiële diensten en digitale dienstverlener, alsook van meldingen vanuit andere landen;
 - Sectorale Overheden⁴ & Sectorale Computer Security Incident Response Teams (hierna "SCSIRT"), die binnen hun sector belast zijn met het toezicht op de uitvoering van de bepalingen van het Ontwerp;

¹ Het betreft bijvoorbeeld elektriciteitsbedrijven, waterleveranciers, luchtvaartmaatschappijen, Kredietinstellingen, zorginstellingen, enz. (zie bijlage 1 bij het Ontwerp).

² P. 1 t.e.m. 3 van de Memorie van Toelichting bij het Ontwerp.

³ Zie artikel 7 van het Ontwerp.

⁴ Zij zullen o.a. instaan voor de identificatie van de aanbieders van essentiële diensten binnen hun sector (cf. artikel 11 Ontwerp).

- Een autoriteit die belast is met *“de actualisering van de nationale strategie voor de beveiliging van netwerk –informatiesystemen”*⁵;
 - Inspectiediensten die toezien op de naleving van het Ontwerp en haar uitvoeringsbesluiten door de aanbieders van essentiële diensten of digitale dienstverleners.
4. In de context van het Ontwerp zullen (minstens) de volgende gegevensverwerkingen plaatsvinden:
- algemene informatie-uitwisseling vanuit de aanbieders van essentiële diensten en digitale dienstverleners naar de in randnummer 3 bedoelde autoriteiten en vanuit laatstgenoemde autoriteiten naar andere (buitenlandse) autoriteiten⁶;
 - verwerken van informatie die de in randnummer 3 opgesomde autoriteiten ontvangen vanwege de aanbieders van essentiële diensten en vanuit de digitale dienstverleners
 - bij de aanmelding van hun *“contactpunt voor de computerbeveiliging”*⁷;
 - in het kader van meldingen van incidenten⁸;
 - verwerkingen door de inspectiediensten⁹ (cf randnummer 3, laatste bullet) in het kader van het toezicht op de aanbieders van essentiële diensten en digitale dienstverleners en dit met name voor wat betreft de naleving van de beveiligingsvereisten of de eisen inzake het melden van incidenten. Artikel 44 van het Ontwerp verschaft deze inspectiediensten ruime onderzoeksbevoegdheden. Ze kunnen met name *“overgaan tot elk onderzoek, elke controle en elk verhoor”* en ze kunnen alle inlichtingen inwinnen die zij nodig achten voor de uitoefening van hun opdracht¹⁰;
 - verwerkingen door de Hoven en Rechtbanken (bij strafrechtelijke procedures) of door de *“sectorale overheden”*¹¹ (bij administratiefrechtelijke procedures) in het kader van de sanctionering van inbreuken op het Ontwerp;
 - verwerkingen door het NCSIRT en de SCSIRT in het kader van het beheer van veiligheidsincidenten¹².

II. ONDERZOEK VAN DE ADVIESAANVRAAG

⁵ Artikel 10, §1, van het Ontwerp.

⁶ Artikel 9 van het Ontwerp.

⁷ Artikelen 23 & 34 van het Ontwerp.

⁸ Artikelen 24 e.v. & 35 e.v. van het Ontwerp.

⁹ -Zie randnummer 3, laatste bullet.

-Zie Titel 4: Hoofdstuk 1, afdeling 2 & Hoofdstuk 2 van het Ontwerp.

1. Algemene opmerkingen

5. De Autoriteit staat heel positief ten aanzien van de *ratio legis* van het Ontwerp: welbepaalde netwerk –en informatiesystemen die van belang zijn voor de openbare veiligheid zo goed mogelijk beveiligen. Zoals de Memorie van Toelichting bij het Ontwerp (p. 3) correct aangeeft, sluit een dergelijk beheer van veiligheidsrisico's aan bij het opzet van de AVG.

6. Zij staat ook gunstig ten aanzien van de samenwerkingsplicht tussen de in randnummer 3 opgesomde instanties en de Autoriteit¹³, alsook ten aanzien van het gemeenschappelijk platform dat zal gecreëerd worden om incidenten te melden¹⁴. Specifiek ten aanzien van voornoemd meldingsplatform, vestigt de Autoriteit er wel de aandacht op dat er – gelet op het in de AVG vervatte principe van de 'verantwoordingsplicht' – bij de uitbouw van dit platform dient over gewaakt te worden dat het de verantwoordelijkheid van de verwerkingsverantwoordelijke blijft om te beslissen bij welke instantie(s) hij een melding doet en bij welke niet. De realisatie van dit platform kan met andere woorden niet tot gevolg hebben dat deze verantwoordelijkheid van de verwerkingsverantwoordelijke wordt 'verschoven' naar één of meerdere instanties die via dit platform meldingen ontvangen.

7. Verder wijst de Autoriteit er op dat er in de praktijk tal van raakvlakken zullen opduiken tussen de bepalingen in het Ontwerp en de regels inzake dataproductie. In dit verband onderlijnt de Autoriteit ook dat de AVG onverminderd van toepassing blijft op verwerkingen van persoonsgegevens die in de context van het Ontwerp zullen plaatsvinden. Alle actoren die onderworpen zijn aan de bepalingen in het Ontwerp, zullen dus – voor zover zij persoonsgegevens verwerken – tegelijk rekening moeten houden met de regelgeving inzake dataproductie. Nochtans zouden zij verkeerdelijk de indruk kunnen krijgen dat ze volledig legaal handelen indien ze enkel de regels in het Ontwerp respecteren terwijl ze misschien de AVG uit het oog verliezen. De Autoriteit pleit er daarom voor om
 - in het Ontwerp een bepaling op te nemen die het principe vastlegt dat het Ontwerp geen afbreuk doet aan de AVG en de daarbij horende nationale uitvoeringswetten¹⁵;

¹⁰ Artikel 44, §3, 3°, van het Ontwerp.

¹¹ Zie randnummer 3, derde bullet.

¹² Zie Titel 5 van het Ontwerp.

¹³ Artikel 8, §2, van het Ontwerp. De artikelen 48 & 52 van de wet van 3 december 2017 *tot oprichting van de Gegevensbeschermingsautoriteit* laat de Autoriteit overigens ook toe om in onderhavige context samen te werken met andere actoren.

¹⁴ Artikel 31, §1, laatste lid & artikel 36, §3, van het Ontwerp.

¹⁵ Artikel 2 van de Richtlijn lijkt dit toe te laten, aangezien deze bepaling verwijst naar de klassieke regels inzake dataproductie (met name naar de oude Richtlijn 95/46/EG, die intussen door de AVG vervangen werd) voor wat de verwerking van persoonsgegevens betreft die in onderhavige context zullen plaatsvinden.

- in de Memorie van Toelichting bij het Ontwerp te wijzen op specifieke gelijkenissen en verschillen tussen de regels in het Ontwerp en de verplichtingen in de AVG¹⁶.

2. Doeleinde

8. Volgens artikel 5.1.b) AVG is de verwerking van persoonsgegevens enkel toegestaan voor welbepaalde uitdrukkelijk omschreven en gerechtvaardigde doeleinden. De Autoriteit stelt vast dat het Ontwerp een – weliswaar algemeen - duidelijk en legitiem doel beoogt: ervoor zorgen dat technische –en organisatorische beveiligingsmaatregelen worden genomen door de aanbieders van essentiële diensten om incidenten te voorkomen of de impact ervan te beperken, teneinde de continuïteit van essentiële diensten te waarborgen. Tegelijk pleit de Autoriteit ervoor om de subfinaliteit van elke aparte categorie van verwerkingen (cf. randnummer 4), expliciet in het Ontwerp op te nemen (cf. randnummer 12).

3. Rechtsgrondslag

9. Elke verwerking van persoonsgegevens moet steunen op een rechtsgrondslag in de zin van artikel 6 AVG. Bovendien is de verwerking van persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten aan strikte voorwaarden onderworpen (artikel 10 AVG).
10. Voor de verwerking van persoonsgegevens die niet behoren tot de bijzondere categorieën van artikelen 9 & 10 AVG, kan het Ontwerp wellicht steunen op de volgende twee rechtsgronden:
 - artikel 6.1.c) voor wat de verwerkingen betreft die uitgevoerd worden door de aanbieders van essentiële diensten en de digitale dienstverleners. Zij delen immers bepaalde persoonsgegevens mee aan de actoren bedoeld in randnummer 3, omdat ze hiertoe verplicht worden door het Ontwerp;
 - artikel 6.1. e) AVG voor wat de verwerkingen betreft die worden verricht door de actoren bedoeld in randnummer 3. Zij vervullen immers een taak van algemeen belang.

¹⁶ Ter illustratie:

- De artikelen 24 e.v. & 35 e.v. van het Ontwerp leggen een meldingsplicht op voor beveiligingsincidenten, terwijl de artikelen 33 & 34 AVG in een meldingsplicht voorzien voor *“inbreuken in verband met persoonsgegevens”*;
- Artikel 23, §1, van het Ontwerp voorziet in een aanmeldingsplicht voor het *“contactpunt voor de beveiliging van netwerk –en informatiesystemen”* en artikel 37.7 AVG bepaalt dat de contactgegevens van de functionaris voor gegevensbescherming aan de toezichhoudende autoriteit moeten medegedeeld worden.

11. De Autoriteit vestigt hierbij de aandacht op artikel 6.3 AVG dat -in samenlezing met artikel 8 EVRM en artikel 22 van de Grondwet-¹⁷ voorschrijft dat regelgeving die de verwerking van persoonsgegevens omkadert, in principe minstens volgende essentiële elementen van die verwerking zou moet vermelden:
- het doel van de verwerking;
 - de types of categorieën van te verwerken persoonsgegevens;
 - de betrokkenen;
 - de entiteiten waaraan en doeleinden waarvoor de persoonsgegevens mogen worden verstrekt;
 - opslagperioden;
 - evenals de aanduiding van de verwerkingsverantwoordelijke.
12. Het Ontwerp dient in voormelde zin te worden gepreciseerd en aangevuld. Dit zou bijvoorbeeld kunnen door in Titel 6 van het Ontwerp een artikel op te nemen waarin per type verwerking (zie hoger randnummer 4) minstens het doel van de verwerking wordt gepreciseerd. Ook de andere essentiële elementen van de verwerkingen moeten in deze nieuwe bepaling worden opgenomen tenzij hiervoor in een delegatie aan de Koning zou worden voorzien.
13. Hierbij aansluitend vestigt de Autoriteit ook de aandacht op artikel 20 van de Kaderwet inzake dataprotectie¹⁸, dat aan federale overheden¹⁹ de verplichting oplegt om protocolakkoorden af te sluiten voor gegevensuitwisselingen die op artikel 6.1.e) AVG gebaseerd zijn.
14. Verder stelt de Autoriteit vast dat er ook gegevens zullen worden verwerkt betreffende strafrechtelijke veroordelingen en strafbare feiten²⁰, wat verwerkingen betreft die krachtens artikel 10 AVG enkel toegestaan zijn onder toezicht van een overheid (of indien de verwerking is toegestaan bij Unierechtelijk of lidstaatrechtelijke bepalingen die passende waarborgen voor de rechten en vrijheden van de betrokkenen bieden). *In casu* zal de verwerking van dit type gegevens uitgevoerd worden onder toezicht van een overheid, met name de actoren bedoeld in randnummer 3, wat strookt met artikel 10 AVG. Deze bepaling uit de AVG dient overigens

¹⁷ Zie arresten van het Grondwettelijk Hof: Arrest nr. 44/2015 van 23 april 2015 (p. 63), Arrest nr. 108/2017 van 5 oktober 2017 (p. 17) en Arrest nr. 29/2018 van 15 maart 2018 (p. 26).

¹⁸ Wet van 30 juli 2018 *betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens*

¹⁹ Een Vlaams Decreet legt overigens gelijkaardige verplichtingen op aan Vlaamse Overheidsdiensten (Cf Artikel 16 van het decreet van 8 juni 2018 *houdende de aanpassing van de decreten aan de 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)*)

²⁰ Zie bv. artikel 54, eerste lid, van het Ontwerp: de procureur des Konings zal de sectorale overheid inlichten wanneer strafrechtelijke vervolging is ingesteld.

eveneens samengelezen te worden met de artikelen 6 AVG²¹, 22 GW en 8 EVRM, wat impliceert dat – ook al vindt de verwerking van dit type van gegevens plaats onder toezicht van een overheid – de essentiële elementen van de verwerking van dit type van gegevens eveneens in de regelgeving dienen vastgelegd te worden, wat *in casu* nog onvoldoende het geval is (zie randnummers 11-12).

4. Principe van de minimale gegevensverwerking

15. Artikel 5.1.c) AVG bepaalt dat persoonsgegevens beperkt moeten zijn tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt (“minimale gegevensverwerking”).
16. De Autoriteit constateert vooreerst dat in artikel 9, §3, laatste lid, van het Ontwerp²² het principe is opgenomen dat uitgewisselde informatie beperkt dient te worden tot *“hetgeen relevant is voor en evenredig is met het doel van die uitwisseling”*. De Autoriteit adviseert om een gelijkaardige bepaling toe te voegen aan Titel 6 van het Ontwerp, opdat deze regel een transversale werking zou krijgen. Er zijn immers nog andere bepalingen in het Ontwerp die gegevensverwerkingen impliceren – zie bijvoorbeeld de artikelen 29, 37, §1, & 62, tweede lid, - waarvoor het vanuit dataprotectie-oogpunt een meerwaarde zou betekenen mochten zij expliciet aan hetzelfde beginsel onderworpen zijn.
17. Verder vestigt de Autoriteit er de aandacht op dat het principe van de “minimale gegevensverwerking” ook impliceert dat wanneer een bepaald doeleinde kan gerealiseerd worden zonder dat hierbij persoonsgegevens worden verwerkt, er voor deze piste dient gekozen te worden. De instanties opgesomd in randnummer 3 dienen zich hier terdege bewust van te zijn en daarom kan het nuttig zijn om hier melding van te maken in de Memorie van Toelichting bij het Ontwerp.

5. Bewaartermijn

18. Volgens artikel 5.1.e) AVG mogen persoonsgegevens niet langer worden bewaard, in een vorm die het mogelijk maakt de betrokkenen te identificeren, dan noodzakelijk voor de verwezenlijking van de doeleinden waarvoor zij worden verwerkt. Het Ontwerp voorziet enkel voor verwerkingen betreffende inbreuken in een welbepaalde bewaartermijn (cf infra

²¹ Zie overweging 51 AVG: “(...) Naast de specifieke voorschriften voor die verwerking [van gevoelige gegevens] dienen de algemene beginselen en andere regels van deze verordening te worden toegepast, met name wat betreft de voorwaarden voor rechtmatige verwerking. (...)”

Zie ook p. 15 van het advies 06/2014 van de Groep *on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*:

²² Zie randnummer 4, eerste bullet.

randnummer 22, bullet 6). De Autoriteit adviseert om voor de andere verwerkingsfinaliteiten – ofwel in het Ontwerp, ofwel in een uitvoeringsbesluit – alsnog in specifieke bewaartermijnen of afbakeningscriteria voor de bewaartermijnen te voorzien.

6. Verantwoordelijkheid

19. Artikel 4.7 AVG bepaalt dat voor de verwerkingen waarvan de regelgeving het doel en de middelen vastlegt, de verwerkingsverantwoordelijke diegene is die de wetgeving in kwestie aanduidt. Het Ontwerp duidt geen verwerkingsverantwoordelijken aan en de Autoriteit adviseert om deze leemte op te vullen (bv. in Titel 6 van het Ontwerp).
20. De Autoriteit stelt verder vast dat de aanbieders van essentiële diensten, de digitale dienstverleners, alsook de autoriteiten opgesomd in randnummer 3, krachtens het Ontwerp allen een functionaris voor gegevensbescherming moeten aanduiden²³ en zij staat evident positief ten aanzien van deze maatregel.

7. Rechten van de betrokkenen

21. Artikel 23 AVG laat de lidstaten toe om binnen welbepaalde grenzen en voor specifieke doeleinden te voorzien in uitzonderingen op de rechten van betrokkenen. De specifieke doeleinden waarvoor dit mogelijk is, staan opgesomd in artikel 23.1 AVG. Iedere wettelijk maatregel die voorziet in beperkingen op de rechten van de betrokkene, moet ten minste specifieke bepalingen bevatten betreffende de elementen opgesomd in artikel 23.2 AVG zoals:
- de doeleinden van de (categorieën van de) verwerking,
 - de categorieën van persoonsgegevens,
 - het toepassingsgebied van de beperkingen,
 - waarborgen ter voorkoming van misbruik of onrechtmatige toegang of doorgifte,
 - specificatie van de (categorieën van) verwerkingsverantwoordelijke(n),
 - de opslagperiodes,
 - de risico's voor de rechten en vrijheden van de betrokkenen en
 - het recht van de betrokkene op kennisgeving inzake de beperking.
22. De Autoriteit analyseert hierna in hoeverre deze voorwaarden gerespecteerd worden:
- wat het doeleinde van de verwerking betreft: In het kader van *“het melden van incidenten”* en in het kader van *“het toezicht bedoeld in Titel 4 van het Ontwerp”*, worden door het Ontwerp alle rechten bedoeld in de artikelen 12 t.e.m. 22 AVG

²³ Artikel 66 van het Ontwerp. De Autoriteit meent overigens dat dit artikel beter net voor artikel 65 van het Ontwerp zou geplaatst worden, aangezien het nu is ondergebracht tussen twee artikelen die over een ander onderwerp handelen (met name over de beperking van de rechten van de betrokkene).

uitgesloten²⁴. De Autoriteit merkt op dat de omschrijving van het doeleinde *“het toezicht bedoeld in Titel 4 van het Ontwerp”* nauwkeuriger zou moeten uitgewerkt worden. Dit zou bijvoorbeeld kunnen door naar de exacte artikels in het Ontwerp te verwijzen waarin de verwerkingen vervat liggen die onderhevig zijn aan de beperkingen van de rechten die in artikel 65 van het Ontwerp zijn vastgelegd. De Autoriteit herinnert er volledigheidshalve aan dat deze beperkingen binnen de grenzen van het strikt noodzakelijke dienen te blijven²⁵;

- wat de categorieën van persoonsgegevens betreft: *“alle categorieën van persoonsgegevens die door de verwerkingsverantwoordelijke(n) worden verwerkt voor de [hogervermelde] doeleinden”*²⁶; De Autoriteit dringt er op aan om deze omschrijving te verduidelijken.
- wat het toepassingsgebied van de beperkingen betreft: Het Ontwerp voorziet ter zake niets en deze leemte dient aldus de Autoriteit te worden opgevuld. Ter illustratie verwijst de Autoriteit naar randnummer 41 van advies nr. 34/2018²⁷.
- wat de waarborgen ter voorkoming van misbruik of onrechtmatige toegang of doorgifte betreft:
 - *“Elke verwerkingsverantwoordelijke moet passende maatregelen nemen om elke vorm van misbruik of onrechtmatige toegang of overdracht van voormelde persoonsgegevens te voorkomen”*²⁸. De Autoriteit verzoekt de aanvrager om (bv. in de Memorie van Toelichting) te expliciteren welke concrete “passende maatregelen” zullen genomen worden om onrechtmatige toegang te vermijden;
 - *“De functionaris voor gegevensbescherming vermeldt de feitelijke en juridische redenen waarop zijn beslissing steunt en deze inlichtingen worden ter beschikking gehouden van de bevoegde toezichthoudende autoriteit”*²⁹. Deze procedure lijkt echter enkel te gelden voor beperkingen op het recht op rectificatie wat dus onvoldoende is (cf. infra randnummer 23);

²⁴ Artikel 65, §2, van het Ontwerp.

²⁵ Cf. randnummer 38 van advies nr. 34/2018.

²⁶ Artikel 65, § 4, van het Ontwerp.

²⁷ “ (...) Wat het toepassingsgebied van de beperkingen betreft:

- *gedurende de periode waarin de betrokkene het voorwerp uitmaakt van een controle of onderzoek (incl. de voorbereidende werkzaamheden van max 1 jaar na ontvangst van het verzoek tot uitoefening van het recht) en gedurende de periode om vervolgingen hieromtrent in te stellen;*
- *voor zover de uitoefening van de rechten nadelig zou zijn voor de controle, het onderzoek of de voorbereidende werkzaamheden of het geheim van het strafonderzoek dreigt te schenden. (...)”*

²⁸ Artikel 65, §4, van het Ontwerp.

²⁹ Artikel 67, §3, tweede lid, van het Ontwerp.

- wat de specificatie van de verwerkingsverantwoordelijken betreft: de aanbieder van essentiële diensten, de digitale dienstverlener of de autoriteiten bedoeld in randnummer 3³⁰;
- wat de opslagperiodes betreft: de gegevens betreffende inbreuken mogen niet langer bewaard worden dan noodzakelijk is voor de vooropgestelde doeleinden en maximaal voor de duur van de verjaringstermijnen³¹. De artikels van het Ontwerp waarnaar hierbij verwezen wordt bevatten echter geen verjaartermijnen. De Autoriteit verzoekt dan ook om voor iedere verwerking de termijnen expliciet in het Ontwerp op te nemen.
- wat de risico's voor de rechten en vrijheden van de betrokkenen betreft:
 - De functionaris voor gegevensbescherming informeert de betrokkene over de mogelijkheid om klacht in te dienen bij de bevoegde toezichthoudende overheid of om een juridictioneel beroep in te stellen³²;
 - De functionaris voor gegevensbescherming vermeldt de feitelijke en juridische redenen waarop zijn beslissing steunt en deze inlichtingen worden ter beschikking gehouden van de bevoegde toezichthoudende overheid³³;

De Autoriteit merkt op dat deze procedures enkel lijken te gelden voor beperkingen op het recht op rectificatie (cf. infra randnummer 23).

Zij adviseert verder om in artikel 67 van het Ontwerp ook een bepaling op te nemen die stipuleert dat de functionaris voor gegevensbescherming de betrokkene onverwijld in kennis stelt van de opheffing van een beperking en dit onmiddellijk na afsluiting van controle of onderzoek (tenzij het dossier wordt overgemaakt aan het openbaar ministerie of aan de bevoegde instelling om over de bevindingen van het onderzoek te beslissen).

- wat het recht van de betrokkene op kennisgeving inzake de beperking betreft: In dit verband zijn twee bepalingen uit het Ontwerp relevant:
 - *“De functionaris voor gegevensbescherming van de verwerkingsverantwoordelijke informeert de betrokkene schriftelijk en dit onverwijld, en in ieder geval binnen een maand na ontvangst van het verzoek, over iedere weigering of beperking van zijn recht op rectificatie, alsook over de redenen voor deze weigering of beperking. De Informatie over de weigering of beperking kan achterwege worden gelaten wanneer de*

³⁰ Artikel 65, §3, van het Ontwerp.

³¹ Artikel 65, §5, van het Ontwerp.

³² Artikel 67, §3, eerste lid, van het Ontwerp.

³³ Artikel 67, §3, tweede lid, van het Ontwerp.

*verstrekking ervan een van de doelstellingen vermeld in artikel 65 zou ondermijnen.*³⁴

- o de verwerkingsverantwoordelijke kan de betrokkene toegang verlenen tot *“beperkte informatie”* over de verwerking van zijn persoonsgegevens, *“voor zover deze kennisgeving de verwezenlijking van de doelstellingen van deze wet niet in het gedrang brengt.”*³⁵

De Autoriteit heeft dienaangaande twee opmerkingen:

- o Ten eerste stelt zij zich de vraag wat met *“beperkte informatie”* bedoeld wordt. Een verduidelijking in het Ontwerp zou dit kunnen ophelderen;
- o Ten tweede verzoekt zij om de inhoud en draagwijdte van de zinsnede *“de doelstellingen van deze wet”* en de *“de doelstellingen vermeld in artikel 65”* te verduidelijken.

23. Verder vestigt de Autoriteit er in het algemeen de aandacht op dat de redactie van artikel 67 van het Ontwerp dient bijgestuurd te worden. De eerste paragraaf stipuleert dat betrokkenen *“een verzoek in verband met hun rechten”* kunnen richten tot de functionaris voor gegevensbescherming, terwijl de tweede en derde paragraaf de procedure beschrijft die deze functionaris hierbij dient te volgen. Deze procedure lijkt echter te worden beperkt tot de gevallen waarin een betrokkene zijn recht op rectificatie (artikel 16 AVG) uitoefent. De Autoriteit verzoekt bijgevolg om deze procedure ook te laten gelden voor de gevallen waarin betrokkenen andere AVG-rechten dan het recht op rectificatie wensen uit te oefenen. Zoniet zijn de hoger geschetste waarborgen (randnummer 22, bullets 4, 7 & 8) niet op deze gevallen van toepassing en beantwoorden deze beperkingen aldus helemaal niet aan de vereisten van artikel 23 AVG.

24. Om de redactie van de artikelen 65 en 67 van het Ontwerp in bovengenoemde zin te verbeteren, zou overigens inspiratie kunnen gevonden worden in de artikelen 59 e.v. van de wet *tot oprichting van het informatieveiligheidscomité en tot wijziging van diverse wetten betreffende de uitvoering van Verordening (EU) 2016/679 van 27 april 2016 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 en tot intrekking van Richtlijn 95/46/EG.*

25. Tot slot stelt de Autoriteit ook vast dat de meldingsplicht vervat in artikel 34 AVG wordt beperkt, met name in artikel 67, §5, van het Ontwerp. Er wordt niet gemotiveerd waarom

³⁴ Artikel 67, §2, van het Ontwerp.

³⁵ Artikel 67, §4, van het Ontwerp.

deze afwijking noodzakelijk zou zijn. De redactie van artikel 67, §5, is bovendien niet duidelijk, aangezien eveneens dezelfde vage zinsnede ("*de doelstellingen van deze wet*") wordt gebruikt die hoger in randnummer 22, bullet 8, reeds wordt bekritiseerd. Daarenboven stemt de tekst van deze bepaling niet overeen met de uitleg die er in de Memorie van Toelichting (p. 35) aan gegeven wordt. In de Memorie staat namelijk dat er toestemming nodig is van de toezichthoudende autoriteit vooraleer een verwerkingsverantwoordelijke zou ontslaan worden van de meldingsplicht vervat in artikel 34 AVG, terwijl deze voorwaarde niet blijkt uit de tekst van artikel 67, §5. De Autoriteit dringt er dan ook op aan om deze bepaling grondig te herwerken.

III. BESLUIT

26. Op voorwaarde dat de volgende opmerkingen in de tekst worden geïntegreerd:

- de betrokken actoren via (de Memorie van Toelichting bij) het Ontwerp sensibiliseren opdat de gegevensverwerkingen die ingevolge het Ontwerp zullen plaatsvinden AVG-conform zouden zijn (zie randnummer 7);
- alle essentiële elementen van de geplande gegevensverwerkingen in het Ontwerp integreren (zie randnummers 11, 12, 14, 18 & 19);
- het principe van de "minimale gegevensverwerking" nog meer implementeren in (de Memorie van Toelichting bij) het Ontwerp (zie randnummers 16 & 17);
- de artikelen 65 & 67 van het Ontwerp herwerken conform de suggesties in de randnummers 22 t.e.m. 25.

is de Autoriteit van oordeel dat het Ontwerp voldoende waarborgen biedt wat de bescherming van de persoonsgegevens van de betrokkenen betreft.

OM DEZE REDENEN

Brengt de Autoriteit een **gunstig advies** uit over het wetsontwerp *tot vaststelling van een kader voor de beveiliging van netwerk –en informatiesystemen van algemeen belang voor de openbare veiligheid* en dit onder de uitdrukkelijke voorwaarde dat voormelde opmerkingen bijkomend worden geïntegreerd.

De Wnd. Administrateur,

De Voorzitter,

(get.) An Machtens

(get.) Willem Debeuckelaere