**Advies nr. 132/2018 van 28 november 2018**

**Betreft:** ontwerp van wet tot wijziging van de wet van 17 juni 2016 inzake overheidsopdrachten, de wet van 17 juni 2016 betreffende de concessieovereenkomsten en de wet van 13 augustus 2011 inzake overheidsopdrachten en bepaalde opdrachten voor werken, leveringen en diensten op defensie- en veiligheidsgebied (CO-A-2018-122)

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 de Staatssecretaris belast met de Administratieve Vereenvoudiging ontvangen op 1 oktober 2018;

Gelet op het verslag van de voorzitter;

Brengt op 28 november 2018 het volgend advies uit:

## I. ONDERWERP EN CONTEXT VAN DE ADVIESAANVRAAG

1. De Autoriteit ontving op 1 oktober 2018 een adviesaanvraag van de Staatssecretaris belast met de Administratieve Vereenvoudiging betreffende een ontwerp van wet tot wijziging van de wet van 17 juni 2016 inzake overheidsopdrachten, de wet van 17 juni 2016 betreffende de concessieovereenkomsten en de wet van 13 augustus 2011 inzake overheidsopdrachten en bepaalde opdrachten voor werken, leveringen en diensten op defensie- en veiligheidsgebied (hierna "het ontwerp").

2. Het ontwerp beoogt een aanpassing van drie wetten ingevolge de omzetting van Richtlijn 2014/55/EU van 16 april 2014 van het Europees Parlement en de Raad inzake elektronische facturering bij overheidsopdrachten[1]. Deze drie wetten zijn de volgende:

- de wet van 17 juni 2016 *inzake overheidsopdrachten*;
- de wet van 17 juni 2016 *betreffende de concessieovereenkomsten*;
- de wet van 13 augustus 2011 *inzake overheidsopdrachten en bepaalde opdrachten voor werken, leveringen en diensten op defensie- en veiligheidsgebied*.

## II. CONTEXT VAN HET ONTWERP

3. Het voorliggende ontwerp kadert in de uitvoering van de Europese wetgeving die tot doel heeft om een Europese standaard te ontwikkelen bij de elektronische facturering van overheidsopdrachten.

4. De Europese Toezichthouder voor gegevensbescherming heeft op 11 november 2013 reeds een advies[2] uitgebracht in deze aangelegenheid met relevante aanbevelingen voor het waarborgen van een toereikende gegevensbescherming bij de toepassing van de voormelde Europese wetgeving.

5. Samen met de aanvullende beginselen van de Verordening (EU) 2016/679[3] (hierna “AVG”) moeten die aanbevelingen voor ogen worden gehouden door de wetgever wanneer er door aanbestedende diensten en aanbestedende instanties persoonsgegevens worden verwerkt. Er moet met name duidelijk worden gesteld dat bestaande wetten inzake gegevensbescherming ook gelden op het gebied van elektronische facturering en dat de bekendmaking van persoonsgegevens ten behoeve van transparantie en aansprakelijkheid moet stroken met de bescherming van de privacy[4].

---

[1] PB, *L 133, 6.5.2014.*
[2] https://edps.europa.eu/sites/edp/files/publication/13-11-11_electronic_invoicing_en.pdf.
[3] 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.*
[4] Overweging 36 van de Richtlijn 2014/55/EU.

## III. INHOUD VAN HET ONTWERP

6. Het ontwerp bevat diverse bepalingen aangaande het elektronisch versturen van facturen aan de aanbestedende overheden en overheidsbedrijven (artikelen 6, 9, 14, 17, 20 en 24 van het ontwerp).

## IV. ONDERZOEK VAN HET ONTWERP

### 1. Toepasselijkheid van de AVG

7. De voormelde Richtlijn 2014/55/EU stelt in haar overweging nr. 20: "*Omdat elektronische facturen persoonsgegevens kunnen bevatten, moet de Commissie ook verlangen dat de Europese norm voor elektronische facturering rekening houdt met de bescherming van persoonsgegevens overeenkomstig Richtlijn 95/46/EG van het Europees Parlement en de Raad alsmede de beginselen van gegevensbescherming door middel van ontwerp, evenredigheid en gegevensminimalisatie*."

8. Actueel werd de Richtlijn 95/46/EG vervangen door de AVG, waarbij de voormelde dataprotectiebeginselen werden overgenomen in de artikelen 5 en 25 AVG, en aangevuld met nieuwe verplichtingen en beginselen.

9. De Autoriteit bekijkt hierna enkel de bepalingen van het ontwerp die betrekking hebben op een verwerking van persoonsgegevens.

### 2. Verwerkte gegevens – beginsel van minimale gegevensverwerking

10. De artikelen 4, 11 en 19 van het ontwerp voegen een nieuwe definitie in van "kernelementen van een elektronische factuur"[5] in de voormelde drie wetten. De artikelen 7, 15 en 21 van het ontwerp bevatten een gelijkaardige bepaling die stelt dat de elektronische factuur minimaal de volgende kernelementen bevat die zijn overgenomen uit de voormelde Richtlijn 2014/55/EU:

*"1° proces- en factuurkenmerken;*
*2° de factuurperiode;*
*3° informatie over de verkoper;*
*4° informatie over de koper;*
*5° informatie over de begunstigde van de betaling;*
*6° informatie over de fiscaal vertegenwoordiger van de verkoper;*
*7° een verwijzing naar de overeenkomst;*
*8° leveringsdetails (bv. adres);*

[5] "*een verzameling van essentiële gegevenscomponenten die een elektronische factuur moet bevatten om grensoverschrijdende interoperabiliteit mogelijk te maken, met inbegrip van de gegevens die nodig zijn om de naleving van de wettelijke voorschriften te waarborgen*."

*9° betalingsinstructies;*
*10° informatie over kortingen of toeslagen;*
*11° informatie over de factuurposten;*
*12° totalen op de factuur;*
*13° de uitsplitsing van de btw per tarief.".*

11. De Autoriteit is van oordeel dat het woord "minimaal" in de gelijkaardig geformuleerde artikelen 7, 15 en 21 van het ontwerp geen extensieve interpretatie kan krijgen, nu vnl. de kernelementen 3 tot en met 6 betrekking kunnen hebben op een verwerking van persoonsgegevens die dient bij uitstek te voldoen aan het **beginsel van minimale gegevensverwerking** vermeld in artikel 5 1. c) AVG[6]. De andere informatie (fiscaal, boekhoudkundig,...) kan evenwel ook betrekking hebben op een natuurlijke persoon (bv. de koper, verkoper,...), zodat ook het verwerken van de gegevens onder die velden ook als een verwerking van persoonsgegevens moet worden beschouwd.

12. Het gebruik van vrije velden in elektronische toepassingen voor elektronische facturen met nieuwe kernelementen bij het verwerken van elektronische facturen en het toevoegen van meerdere persoonsgegevens dienen derhalve te worden vermeden omdat zij niet te verenigen zijn met artikel 5.1 c) AVG.

### 3. Finaliteitsbeginsel en bekendmaking, voor transparantie- en boekhouddoeleinden, van persoonsgegevens die in verband met elektronische facturering zijn vergaard

13. Artikel 8 van de Richtlijn 2014/55/EU bevat de volgende inhoudelijke bepalingen:

> *"1.Deze richtlijn laat van toepassing zijnde Unieregelgeving en nationale regelgeving over gegevensbescherming onverlet.*
> *2.Onder voorbehoud van andersluidende bepalingen in Unieregelgeving of nationale regelgeving en onverminderd vrijstellingen en beperkingen vastgelegd in artikel 13 van Richtlijn 95/46/EG, mogen voor elektronische facturering verkregen persoonsgegevens uitsluitend voor dat doel of daarmee vergelijkbare doeleinden worden gebruikt.*
> *3. Onverminderd vrijstellingen en beperkingen vastgelegd in artikel 13 van Richtlijn 95/46/EG zorgen de lidstaten ervoor dat regelingen voor de bekendmaking, voor transparantie- en boekhouddoeleinden, van persoonsgegevens die in verband met elektronische facturering zijn vergaard, stroken met het doel van die bekendmaking en met het beginsel van de bescherming van de privacy."*

[6] "*Persoonsgegevens moeten" (...) "toereik*end zijn, ter zake *dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt*".

14. Het ontwerp zet de punten 2 en 3 van voormeld artikel 8 van de Richtlijn 2014/55/EU om in de artikelen 5 (nieuw artikel 13, § 4 van de wet van 17 juni 2016 *inzake overheidsopdrachten*) en 13 (nieuw artikel 31, § 4 van de wet van 17 juni 2016 *betreffende de concessieovereenkomsten*).

> *"§ 4 . De persoonsgegevens die werden verkregen met het oog op de verwerking van de facturen mogen uitsluitend voor dat doel of daarmee vergelijkbare doeleinden worden gebruikt. De regelingen voor de bekendmaking van persoonsgegevens die in verband met elektronische facturering zijn vergaard, moeten stroken met het doel van die bekendmaking en met het beginsel van de bescherming van de privacy."*

15. Het verklaren in de wetgeving dat het finaliteitsbeginsel moet worden gewaarborgd, betekent uiteraard niet dat dit in de praktijk ook het geval zal zijn. De bepaling dat de bekendmaking moet "stroken met het beginsel van de bescherming van de privacy" is dan wel een letterlijke overname uit de Europese Richtlijn, maar voegt inhoudelijk geen echte waarborg toe. Zeker wat betreft de bekendmaking van persoonsgegevens in verband met elektronische facturering is er geen guidance door de Europese en Belgische wetgever, hetgeen zal zorgen voor een uiteenlopende toepassing en een variabel risico voor de betrokken natuurlijke personen.

16. In de praktijk is het een aandachtspunt om bij publicatie of ander hergebruik voldoende garanties tot bescherming van de betreffende natuurlijke personen te voorzien zoals:

- pseudonimisering[7] en/of anonimisering van persoonsgegevens;
- een verbod op het decoderen van gecodeerde persoonsgegevens;
- afdoende informatie aan de betrokkenen over hun rechten van inzage, rectificatie of bezwaar in geval derden hun persoonsgegevens zouden verwerken met het oog op direct marketing (artikelen 15, 16 en 21 AVG);
- een duidelijke wettelijke basis en waarborgen voor het opstellen van profielen van natuurlijke personen, data-analyses ("data mining") die correlaties zouden aangeven zonder juistheid te garanderen, met mogelijke (rechts)gevolgen die bepaalde bevolkingsgroepen als onverwacht, ongepast of ongewenst ervaren.

17. Of de beginselen van de AVG zullen worden nageleefd zal in belangrijke mate afhangen van de functionaliteiten van de software die wordt gekozen, en hoe met de software wordt omgegaan.

18. Uit de nota aan de ministerraad blijkt dat FOD Beleid en Ondersteuning (hierna "FOD BOSA") een interface ontwikkelde "die toelaat elektronisch ontvangen facturen om te zetten in een leesbare pdf voor de instellingen die nog over een boekhoudsoftware zouden beschikken die geen e-facturen

[7] Artikel 4, 5) AVG en overweging 28 AVG.

kan verwerken". In de mate deze interface wordt toegepast moeten er ook technische waarborgen worden geboden opdat ook bij de toepassing van de functionaliteit van (automatische) leesbaarheid het voormelde beginsel van doelbinding gewaarborgd blijft.

## 4. Risicogebaseerde aanpak onder de AVG en gegevensbeschermingseffectbeoordeling:beoordeling van de kenmerken van software gebruikt voor het verwerken van de kernelementen van elektronische facturen

19. Volgens de AVG[8] moeten de beginselen van **gegevensbescherming door ontwerp** ("privacy by design") en **gegevensbescherming door standaardinstellingen** ("privacy by default") ook bij openbare aanbestedingen in aanmerking worden genomen.

20. De wetgeving zou meer nadruk moeten leggen op de vereiste in de AVG (zgn. "risicogebaseerde aanpak"[9]) tot het beoordelen van de risico's en dataprotectie(on)vriendelijke kenmerken van software en licentievoorwaarden voor de betrokkenen onder de AVG, die eigen zijn aan de meest gebruikte (standaard)pakketten voor facturatie, boekhouding en fiscaliteit.

21. In een aanvullende reactie van 23 oktober 2018 stelde de aanvrager dat alle software mogelijkerwijze betrokken is die inkomende en/of buitengaande facturen verwerkt. Men beschikt actueel niet over een lijst van deze software en de conformiteit van deze software met de AVG was nog niet het voorwerp van een evaluatie.

22. Zonder een gegevensbeschermingseffectenbeoordeling (artikel 35 AVG) waarbij de gebruikte software en licenties grondig worden onderzocht dreigt de voormelde verwijzing naar een deel van de beginselen van de AVG slechts schone schijn te zijn. Dit nu veel toepassingen de basisbeginselen van de AVG niet naleven, dataprotectieverklaringen van licentiegevers weinig transparant zijn en/of licentieverleners al te vlug stellen dat zij "conform de AVG" werken. Een aantal licentiegevers verstrekken persoonsgegevens aan derden vanuit hun commerciële (winstgevende) doeleinden, en/of profileren natuurlijke personen op basis van de inhoud van de communicaties, soms uitgelegd als een "veiligheidsmaatregel". Het gebruik van veel standaardpaketten, modellicenties en/of gratis software voor het verwerken van elektronische factuurgegevens kan bijzondere of ongekende risico's inhouden voor de gebruiker, en standaardfunctionaliteiten zullen hierbij niet altijd voldoende rekening houden met de plichten van verwerkingsverantwoordelijken onder de AVG. Zo worden gegevens vaak in de cloud geplaatst, in landen zonder passend niveau van gegevensbescherming.

[8] Overweging 78 *in fine*.
[9] Zie o.m. artikel 32.1 AVG.

23. Een van de kenmerken die nog te weinig aandacht krijgt is het koppelen van API's ("Application Programming Interfaces") aan de toepassingen voor elektronische facturatie, boekhouding,... via dewelke persoonsgegevens worden verwerkt. Het toepassen van API's kan immers inhouden dat risico's worden verhoogd (incl. risico van niet compliance met relevante beginselen van de AVG zoals bij het verhogen van de deelbaarheid van de gegevens), of dat risico's voor de rechten en vrijheden van de betrokkene worden verlaagd (bv. encryptie, pseudonimisering, aggregatie,...).

24. De Autoriteit acht het derhalve raadzaam dat op federaal vlak periodiek een inventaris en gegevensbeschermingseffectenbeoordeling (lijst van risico's, zwakheden in de software,...) worden opgemaakt. Dit kan gebeuren op het niveau van FOD BOSA alvorens overheidsdiensten hun belangrijkste toepassingen (bv. FEDCOM[10],...) verder ontwikkelen teneinde elektronische facturen te verwerken.

## 5. Betrekken van de functionaris voor gegevensbescherming ("DPO") en transparantie van diens rol

25. In het licht van de verantwoordingsplicht onder artikel 5.2 AVG is de Autoriteit van oordeel dat het verwerken van persoonsgegevens via elektronische facturen steeds moet gebaseerd zijn op weloverwogen keuzes van de leidinggevenden bij de overheidsdiensten (verwerkingsverantwoordelijken).

26. De Autoriteit is van oordeel dat meer aandacht moet worden gegeven aan de rol van de DPO, die betrokken moet worden bij het ontwikkelen van applicaties in deze context. Volgens artikel 38.1 AVG moet de DPO van de verwerkingsverantwoordelijke immers worden betrokken "bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens".

27. Dit impliceert ook dat de DPO (waar nodig ondersteund door een technisch team van FOD BOSA) betrokken moet zijn wanneer keuzes en overwegingen ter beslissing worden voorgelegd aan de leidinggevenden bij de betreffende overheden aangaande de verwerking van persoonsgegevens uit elektronische facturen (keuze voor ICT platform, software,...).

28. In casu ontwikkelde FOD BOSA een applicatie met een functionaliteit die het risico voor de rechten en vrijheden van de betrokkenen (zoals bedoeld onder de AVG) potentieel verhoogt terwijl bij navraag blijkt dat de DPO niet betrokken was bij deze ontwikkeling. De website van de FOD BOSA

[10] De boekhoudsoftware van de federale overheid die facturen ontvangt en verwerkt. Zie de FAQ (https://spp.yourict.be/ucontent/6369c7c90f504f829dbb221697f3b51c_nl-BE/WORD/index.pdf) en helpdesk (contact adres FEDCOM.Helpdesk@bosa.fgov.be).

vermeldt ook niet de mogelijkheid tot en wijze van contactname van en met de DPO, hetgeen in strijd is met de bepalingen in de artikelen 13.1 b), 14.1 b) en 38.4[11] AVG.

29. In een aanvullende reactie van 23 oktober 2018 stelde de aanvrager wel dat de DPO van FOD BOSA zal worden betrokken om de noodzakelijke risicoanalyses te verrichten en dat deze hierover een rapport zal opstellen.

30. Het ontwerp kan concrete inhoudelijke bepalingen voorzien in de voormelde wetten die de rol van de DPO in die zin ondersteunen bij het maken van keuzes aangaande het verwerken van de kernelementen van elektronische facturen.

## IV. BESLUIT

31. De Autoriteit is van oordeel dat de loutere verwijzing naar dataprotectielementen uit de AVG slechts een beperkte (symbolische) waarde heeft (randnummer 15).

32. Indien de wetgever de AVG wenst toe te passen, moet in de aangepaste wetten sterker worden ingezet op het concretiseren van plichten van verwerkingsverantwoordelijken onder de AVG wanneer kernelementen van elektronische facturen worden verwerkt. De basisacties die moeten gebeuren zijn:

- het maken van een inventaris van vaak gebruikte software voor het verwerken van de kernelementen, met een lijst van hun risico's en dataprotectie(on)vriendelijke kenmerken (randnummer 19);
- de periodieke evaluatie van de risico's en kenmerken van de voornaamste toepassingen die worden gebruikt door de overheidsdiensten (bv. FEDCOM,...) via een gegevensbeschermingseffectenbeoordeling (randnummer 23);
- het betrekken van de DPO bij relevante keuzes inzake platformen, software,... via dewelke kernelementen worden verwerkt, en het duidelijker bekend, en het vermelden van de wijze van contactname met de DPO (randnummer 26).

[11] "Betrokkenen kunnen met de functionaris voor gegevensbescherming contact opnemen over alle aangelegenheden die verband houden met de verwerking van hun gegevens en met de uitoefening van hun rechten uit hoofde van deze verordening"

**OM DEZE REDENEN**

Verleent de Autoriteit een gunstig advies over de aangehaalde elementen van het ontwerp, op voorwaarde dat de elementen vermeld in randnummer 31 worden nageleefd.

Spreekt zij zich niet uit over de overige bepalingen van het ontwerp.

De Wnd. Administrateur, De Voorzitter,

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