



Advies nr 58 / 2015 van 16 december 2015

Betreft: adviesaanvraag m.b.t. een ontwerp van koninklijk besluit houdende de elektronische communicatie overeenkomstig artikel 32 *ter Gerechtelijk Wetboek* (CO-A-2015-062)

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 het verzoek om advies van de heer Koen GEENS ontvangen op 16/11/2015;

Gelet op het verslag van de heer Frank DE SMET;

Brengt op 16 december 2015 het volgend advies uit:

I. VOORWERP VAN DE AANVRAAG

1. Artikel 32^{ter} *Gerechtelijk Wetboek*¹, dat in werking treedt op 01/01/2016², bepaalt:

“Elke kennisgeving of mededeling aan of neerlegging bij de hoven of rechtbanken, het openbaar ministerie of diensten die afhangen van de rechterlijke macht, met inbegrip van de griffies en parketsecretariaten, of elke kennisgeving of mededeling aan een advocaat, een gerechtsdeurwaarder of een notaris, door de hoven of rechtbanken, het openbaar ministerie of diensten die afhangen van de rechterlijke macht, met inbegrip van de griffies en parketsecretariaten, of door een advocaat, een gerechtsdeurwaarder of een notaris, kan gebeuren door middel van het informaticasysteem van Justitie dat door de Koning wordt aangewezen.

De Koning bepaalt de nadere regels van dat informaticasysteem, waarbij de vertrouwelijkheid en effectiviteit van de communicatie worden verzekerd.

Het gebruik van het voormelde informaticasysteem kan door de Koning aan de instanties, diensten of actoren vermeld in het eerste lid of sommigen onder hen worden opgelegd.”

2. Het voorgelegde ontwerp van koninklijk besluit (hierna het ontwerp):
 - identificeert 2 informaticasystemen waarop een beroep wordt gedaan, namelijk:
 - o het eBox netwerk voor kennisgevingen, mededelingen en neerleggingen;
 - o het eDeposit systeem dat specifiek is voor het neerlegging van conclusies en stukken;
 - stelt de regels en technieken vast die door deze informaticasystemen dienen te worden gebruikt.

3. Er werd initieel bij hoogdringendheid advies gevraagd binnen een termijn van 15 dagen gelet op de inwerkingtreding op 01/01/2016. De Commissie merkt op dat deze hoogdringendheid – waardoor zij minder tijd heeft om dit dossier ten gronde te bestuderen – moet worden gerelativeerd gezien:

- artikel 32^{ter} *Gerechtelijk Wetboek* voorziet in de mogelijkheid, niet in de verplichting, om kennisgevingen, mededelingen en neerleggingen te verrichten door middel van het informaticasysteem van Justitie. Het verloop van gerechtelijke procedures wordt niet

¹ Ingevoegd door artikel 3 van de wet van 19 oktober 2015 houdende wijziging van het burgerlijk procesrecht en houdende diverse bepalingen inzake justitie.

² Artikel 51, tweede lid, van de wet van 19 oktober 2015.

gehypothekeerd bij gebrek aan uitvoeringsbesluit tegen 01/01/2016 vermits er gewoon kan worden verder gewerkt op de gebruikelijke manier;

- het eBox netwerk niet operationeel zal zijn tegen 01/01/2016 (verklaart waarom artikel 9 van het ontwerp bepaalt dat het besluit in werking treedt op 01/01/2016 maar slechts van toepassing is in de mate dat de informaticasystemen ter beschikking worden gesteld);
- het eDeposit systeem reeds operationeel is (op het niveau van de hoven van beroep). Het ontbreken van een wettelijke basis en uitvoeringsbesluit vormde kennelijk geen beletsel voor de invoering en het gebruik van dit systeem.

II. ONDERZOEK TEN GRONDE

4. De invoering van de mogelijkheid om in de context van een gerechtprocedure kennisgevingen, mededelingen en neerleggingen via een informaticasysteem te verrichten, zal leiden tot de geautomatiseerde verwerking van persoonsgegevens, meer in het bijzonder van gerechtelijke gegevens in de zin van artikel 8 WVP. De bepalingen van de WVP zijn dus van toepassing.

5. Bij de geautomatiseerde verwerking van gerechtelijke gegevens via de aangeduide informaticasystemen zijn betrokken: hoven, rechtbanken, het openbaar ministerie of diensten die afhangen van de rechterlijke macht, de griffies en parketsecretariaten, advocaten, gerechtsdeurwaarders en notarissen. Zij komen allen op basis van artikel 8, § 2, a), b) en d), WVP in aanmerking om dergelijke gegevens te verwerken. De Commissie vestigt volledigheidshalve de aandacht op de toepasselijkheid van artikel 25 van het koninklijk besluit van 13 februari 2001³ op de verwerking van gerechtelijke gegevens.

6. Artikel 1 van het ontwerp wijst 2 informaticasystemen aan: het eBox netwerk en het eDeposit systeem.

A. EBOX NETWERK

³ Koninklijk besluit van 13 februari 2001 *ter uitvoering van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens*.

7. In de bijkomende informatie die werd ontvangen wordt gewag gemaakt van de eJustbox. Teneinde verwarring te vermijden met de eBox⁴ en de eHealthbox⁵ die reeds beschikbaar zijn, suggereert de Commissie om in het ontwerp ook de term eJustbox te gebruiken maar dit staat uiteraard los van de grond van de zaak waarover de Commissie zich dient uit te spreken.

8. Volgens de verstrekte informatie zal het eBox netwerk gebaseerd zijn op dezelfde principes als die van de eHealthbox berichtendienst (zie ook voetnoot 5) dat ter beschikking wordt gesteld aan de actoren in de gezondheidszorg. Het netwerk waarvan sprake in het ontwerp is eveneens een systeem van beveiligde elektronische brievenbussen voor bi-directionele en geadresseerde communicatie – ter beschikking gesteld door de FOD Justitie – waarin de titularis van de eBox berichten kan ontvangen en van waaruit hij berichten kan verzenden (zie artikel 2 van het ontwerpbesluit). Net zoals bij de eHealthbox zal de integriteit van de berichten en de authenticatie van afzender en ontvanger door gepaste technieken (waaronder encryptie) worden verzekerd. Ook zal er gebruik gemaakt worden van logging en time-stamping⁶.

9. De acties die door middel van de eBox worden verricht zijn ten gronde niet nieuw. Wat nieuw is, is de wijze (elektronische implementatie) waarop ze worden uitgevoerd wat op zich uiteraard een gunstige evolutie zou kunnen zijn. Tot op heden gebeurden de in het Gerechtelijk Wetboek voorziene kennisgevingen en mededelingen in de regel op papier via de gewone post of door persoonlijke overhandiging.

10. Rekening houdend hiermee wordt vastgesteld dat het doeleinde van het eBox netwerk welbepaald, uitdrukkelijk omschreven en gerechtvaardigd is (artikel 4, § 1, 2°, WVP).

11. Kennisgevingen en mededelingen bevatten persoonsgegevens. Dit zijn dezelfde dan wanneer de traditionele weg wordt bewandeld. Normaal gezien zijn deze beperkt tot de gegevens die relevant zijn voor de beslechting van het geschil en kan besloten worden dat ze toereikend, ter zake dienend en niet overmatig zijn (artikel 4, § 1, 3°, WVP). In het kader van een gerechtelijke procedure dient te worden aangestipt dat gegevens worden verwerkt die van gevoelige aard zijn (artikel 8, WVP), dewelke een minimum aan garanties qua beveiliging vergen.

⁴ De bestaande eBox-technologie, initieel ontwikkeld voor de sociale zekerheid, werd aangepast met het oog op een veralgemeend gebruik (enkel ontvangen van berichten verzonden door de overheid) door alle Belgische burgers en ondernemingen. Online opslag en toegangscontrole met de elektronische identiteitskaart (voor burgers) zorgen voor een gegarandeerde, vertrouwelijke ontvangst bij de juiste bestemming. De eBox kan worden ingezet door alle overheidsdiensten die dat wensen.

Zie o.a. op <https://www.socialsecurity.be/nl/citizen/static/infos/ebox/transit.htm> (burgers) en https://www.socialsecurity.be/site_nl/general/helpcentre/ebox/transit.htm (ondernemingen).

⁵ De dienst eHealthBox heeft tot doel voor alle actoren in de gezondheidszorg een elektronische en beveiligde brievenbus beschikbaar te stellen die toelaat om berichten te verzenden en te lezen.

Zie o.a. op <https://www.ehealth.fgov.be/nl/support/basisdiensten/beveiligde-elektronische-brievenbus-ehbox>.

⁶ Zie bespreking van artikel 3 in het verslag aan de Koning.

12. In tegenstelling tot de traditionele weg, leidt het gebruik van de eBox ook tot de verzameling van persoonsgegevens over de gebruikers van het systeem. Artikel 3 van het ontwerp, dat handelt over de informaticatechnieken die het systeem gebruikt, maakt gewag van “registreren of loggen”. Dit laatste houdt normalerwijze in dat wordt geregistreerd wie-wanneer-welke actie stelt. Vermits niet nader wordt toegelicht welke gegevens zullen worden geregistreerd, kan de Commissie zich niet uitspreken over de proportionaliteit van de verwerking. Ook m.b.t. de bewaartermijn (artikel 4, § 1, 5°, WVP) is niets gepreciseerd. In het ontwerp is ook nagelaten om een verantwoordelijke voor de verwerking van deze gegevens aan te duiden of de garantie te voorzien van een adequaat en strikt gebruikers- en toegangsbeheer.

13. Hierbij aansluitend stelt de Commissie vast dat het ontwerp nergens een verantwoordelijke voor de verwerking vermeldt noch voor de gegevensverwerkingen via het eBox netwerk, noch voor de gegevensverwerkingen via het eDepositsysteem. Het ontwerp moet op dit punt worden aangevuld.

14. Met betrekking tot de praktische werking van de eBox zijn er een aantal onbeantwoorde vragen:

- het is niet duidelijk of er naast persoonlijke eBox-en – die uitsluitend toegankelijk zullen zijn voor de titularis ervan – ook eBox-en op organisatieniveau zullen mogelijk zijn die medewerkers van een organisatie kunnen raadplegen uit hoofde van hun functie (bv secretariaatsmedewerkers die meestal de inkomende post behandelen (bijvoorbeeld kennisgevingen m.b.t. pleitdata noteren in agenda vooraleer de kennisgeving met dossier klaar te leggen))?
- ook stelt zich de vraag hoe het gebruikers- en toegangsbeheer - dat toelaat gebruikers te identificeren, te authentifieren en hun relevante kenmerken (hoedanigheden), mandaten en toegangsmachtigingen te controleren en te beheren - in praktijk geïmplementeerd is. Zijn er bijvoorbeeld geactualiseerde authentieke bronnen beschikbaar die toelaten om de hoedanigheid van een persoon te controleren? De concrete en gedetailleerde uitwerking van een adequaat en strikt gebruikers- en toegangsbeheer dient evenwel niet in het ontwerp als zodanig te gebeuren, maar de principes dienen wel te worden opgenomen.

15. Artikel 3 van het ontwerp somt op algemene wijze de informaticatechnieken op die het eBox netwerk zal gebruiken met het oog op onder meer het realiseren van de door artikel 16 WVP opgelegde vereisten qua vertrouwelijkheid en beveiliging. Op basis van de handleiding van de eBox die aan de Commissie werd bezorgd⁷, kan zij echter moeilijk beoordelen of het door de FOD Justitie

⁷ Voor eDeposit systeem kon een demonstratiefilm worden geraadpleegd.

geconcipeerde netwerk een passend beveiligingsniveau zal verzekeren rekening houdend met de stand van de techniek enerzijds en de gevoeligheid van de betreffende gegevens anderzijds. De Commissie raadt overigens aan om bij het versturen van elektronische berichten tussen verzender en ontvanger adequate encryptietechnieken te gebruiken om de vertrouwelijkheid van het bericht te garanderen (mag alleen gelezen kunnen worden door de bedoelde ontvanger). Als voorbeeld verwijst ze naar de encryptie als een van de basisdiensten van het eHealth-platform⁸. Artikel 3 van het ontwerp moet als dusdanig op dit vlak worden aangevuld.

16. De Commissie stelt ook vast dat de ontwerptekst van artikel 3 of de erbij horende toelichting in het verslag aan de Koning op een aantal punten voor precisering/verduidelijking vatbaar zijn:

- in het eerste gedachtestreepje wordt gewag gemaakt van “de oorsprong van de zending verzekeren”. Wordt daarmee de identiteit bedoeld van diegene het document heeft verstuurd?
- in het tweede gedachtestreepje wordt gesteld dat de afzender en bestemming ondubbelzinnig worden geïdentificeerd. In het ontwerp moet echter expliciet vermeld worden dat authenticatie ook nodig is (zoals vermeld in het verslag aan de Koning). Identificatie en authenticatie zijn immers 2 verschillende zaken:
 - o identificatie is de vaststelling van de unieke identiteit;
 - o authenticatie is het proces van verificatie waarbij wordt nagegaan of de identiteit die een gebruiker beweert te hebben, hem wel degelijk toebehoort;

Om de toegang tot de eBox door onbevoegden (artikel 16, § 4, WVP) te vermijden volstaat de ondubbelzinnige identificatie dus niet.

17. De technieken vermeld in artikel 3 van het ontwerp zijn identiek aan deze vermeld in artikel 7 van het ontwerp⁹. In het verslag aan de Koning wordt echter alleen bij artikel 7 gewag gemaakt van een two-factor authenticatie¹⁰ van de afzender zonder verdere uitleg. De manier waarop men dit wil implementeren of de motivatie waarom er bij de eBox een minder strenge aanpak zou nodig zijn dan bij eDeposit ontbreekt echter.

18. Artikel 4 van het ontwerp maakt gewag van 3 statussen op het niveau van de ontvanger: gepubliceerd, ontvangen en gelezen. Deze statussen worden gemeld aan de afzender. De exacte definitie van deze statussen ontbreekt echter (wat is bijvoorbeeld het verschil tussen gepubliceerd en

⁸ Artikel 5, 4° van de wet van 21 augustus 2008 *houdende oprichting en organisatie van het eHealth-platform en diverse bepalingen*.

Zie ook <https://www.ehealth.fgov.be/nl/support/basisdiensten/systeem-voor-end-end-vercijfering>

⁹ Dit laatste somt de informaticatechnieken op die door het eDeposit zullen worden gebruikt.

¹⁰ Two factor authentication vereist twee of meer authenticatiemiddelen (factoren), deze zijn: iets wat de gebruiker weet, iets wat de gebruiker heeft, iets wat de gebruiker is.

ontvangen?). De status “gelezen” roept bovendien vragen op wanneer men de toelichting in het verslag aan de Koning leest: *“De e-Box garandeert niet dat de elektronische post effectief gelezen is, desgevallend dat deze geopend is (status “gelezen”), maar wel met de zekerheid dat deze toegekomen is”*. Voor de verzender is het enige wat van belang is dat zijn bericht werd ontvangen. Juridisch gezien is het bovendien niet relevant dat de afzender kennis heeft of het bericht al dan niet geopend of gelezen is. In de mate dat het systeem de opening/lectuur van documenten in de eBox zou monitoren, betreft dit dus een ongerechtvaardigde en disproportionele gegevensverwerking.

B. EDEPOSIT SYSTEEM

19. Lectuur van artikel 1, § 2, en artikel 6 van het ontwerp leert dat door middel van dit systeem conclusies en overtuigingsstukken kunnen worden neergelegd (=opgeladen) in een dossier dat aanhangig is bij een gerecht. Het betreft hier een vorm van niet-geadresseerde en uni-directionele communicatie. Het is dus een dossier-gebonden toepassing op niveau van een bepaalde zaak. Volgens verstrekte informatie is dit systeem op het niveau van de hoven van beroep in burgerlijke zaken al enige tijd operationeel.

20. De acties die door middel van eDeposit worden verricht zijn ten gronde niet nieuw. Wat nieuw is, is de wijze (elektronische implementatie) waarop ze worden uitgevoerd wat op zich uiteraard een positieve evolutie zou kunnen zijn. Tot op heden gebeurde de in het *Gerechtigd Wetboek* voorziene neerlegging van conclusies en stukken in de regel op papier via de gewone post of door persoonlijke overhandiging.

21. Rekening houdend hiermee wordt vastgesteld dat het doeleinde van het eDeposit systeem welbepaald, uitdrukkelijk omschreven en gerechtvaardigd is (artikel 4, § 1, 2°, WVP).

22. Conclusies en overtuigingsstukken bevatten persoonsgegevens. Dit zijn dezelfde dan wanneer voor de neerlegging de traditionele weg bewandeld wordt. Normaal gezien zijn deze beperkt tot deze die relevant zijn voor de beslechting van het geschil en kan besloten worden dat ze toereikend, ter zake dienend en niet overmatig zijn (artikel 4, § 1, 3°, WVP).

23. De bedenkingen/vragen die in de punten 12 tot 17 m.b.t. de eBox werden geformuleerd, gaan bij analogie en indien van toepassing ook op voor het gebruik van het eDeposit systeem. De Commissie verwijst hier ook nog eens expliciet naar het feit dat de vertrouwelijkheid van de gegevens moet worden gegarandeerd door aangepast encryptietechnieken die verzekeren dat stukken enkel door gemachtigde gebruikers kunnen worden gelezen. Artikel 7 van het ontwerp moet als dusdanig op dit vlak worden aangevuld.

24. Momenteel beschikt de Commissie voor wat eDeposit betreft over geen informatie m.b.t. de volgende specifieke punten:

a) uit de demonstratievideo van eDeposit blijkt dat een gebruiker die het systeem wenst te gebruiken voor het opladen van stukken zich moet identificeren en authenticeren aan de hand van zijn eID met pincode (wat positief is). Vervolgens moet hij de hoedanigheid die hij heeft, zelf opgeven (drop down lijst) waarbij men eerder zou verwachten dat het systeem zelf de hoedanigheid nagaat of op zijn minst de hoedanigheid controleert van diegene die zich aanmeldt (door authentieke bronnen te consulteren).

b) gebruikers- en toegangsbeheer:

Wat de "schrijfrechten" in het dossier betreft:

- is de mogelijkheid om stukken op te laden in een dossier beperkt tot een medewerker van het gerecht vermeld in artikel 32 *ter Gerechtelijk Wetboek* van wie gekend is dat hij in dat dossier beroepshalve optreedt? Wordt er hier een authentieke bron van bijgehouden?
- is het opladen van stukken in eDeposit op organisatieniveau mogelijk zodat bijvoorbeeld het administratief personeel van een medewerker van het gerecht vermeld in artikel 32 *ter Gerechtelijk Wetboek* stukken kan neerleggen? Zo ja, onder welke voorwaarden?

Wat de "leesrechten" in het dossier betreft:

- er wordt nergens aangegeven of/hoe de toegang tot de opgeladen stukken en het dossier waarin zij zich bevinden, is geregeld. Deze moet worden beperkt tot medewerkers van het gerecht die in het dossier optreden en tot het "gerechtspersoneel" dat uit hoofde van zijn werkzaamheden bij de behandeling van het dossier betrokken is.

c) het is niet duidelijk waarom in artikel 7 in het tweede gedachtestreepje gewag wordt gemaakt van de identificatie van de bestemming gelet op het feit dat het hier gaat over een vorm van niet-geadresseerde communicatie waar de stukken worden opgeladen in een dossier.

OM DEZE REDENEN, de Commissie

brengt, gelet op de opmerkingen in dit advies,:

- een **gunstig** advies uit over de geplande invoering van het eBox netwerk en het eDeposit syteem, wat als een gunstige evolutie kan worden beschouwd omdat dit in principe een efficiëntere en modernere communicatie tussen de actoren van de rechterlijke macht toelaat met meer garanties

voor onder meer de vertrouwelijkheid en integriteit van de gegevens en een strikt toegangs- en gebruikersbeheer. Deze garanties dienen echter duidelijk te worden opgenomen in het ontwerp.

- een **ongunstig** advies uit voor wat betreft bepaalde aspecten inzake de basisgaranties die beter dienen te worden omkaderd:

- het garanderen van een passend beveiligingsniveau en met name het gebruik van encryptietechnieken voor het verzekeren van de vertrouwelijkheid van de gegevens (randnummers 11, 15 en 23);
- een adequaat en strikt gebruikers- en toegangsbeheer en het bepalen van lees- en schrijfrechten (randnummers 12, 14, 16 en 24);
- aanduiden van de verantwoordelijken voor de verwerking (randnummers 12 en 13);
- specificeren van de bijgehouden gegevens en bewaartermijn betreffende het registreren en loggen (randnummer 12);
- verklaren van het verschil in technieken voor authenticatie tussen eBox en eDeposit (randnummer 17);
- uitklaren van de definitie en relevantie van de verschillende statussen van de berichten op niveau van de ontvanger (randnummer 18).

De Wnd. Administrateur,

De Voorzitter,

(get.) An Machtens

(get.) Willem Debeuckelaere