Advies nr 20/2014 van 19 maart 2014

Betreft: Adviesaanvraag betreffende het ontwerp van Koninklijk besluit tot vaststelling van de voorwaarden, de procedure en de gevolgen van de erkenning van aanmeldingsdiensten voor digitale overheidstoepassingen die gebruik maken van niet-verbonden aanmeldingsmiddelen (CO-A-2014-015)

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 Hendrik Bogaert, staatssecretaris voor Ambtenarenzaken en Modernisering van de Openbare Diensten, ontvangen op 11/02/2014; Gelet op de bijkomende inlichtingen, ontvangen op 27/02/2014;

Gelet op het verslag van de heer Frank Robben;

Brengt op 19 maart 2014 het volgend advies uit:

I. ONDERWERP VAN DE ADVIESAANVRAAG

1. Bij middel van een schrijven d.d. 7 februari 2014 heeft de Staatssecretaris voor Ambtenarenzaken en Modernisering van de Openbare Diensten (hierna 'de aanvrager') de Commissie bij hoogdringendheid om een advies verzocht aangaande het ontwerp van Koninklijk besluit tot vaststelling van de voorwaarden, de procedure en de gevolgen van de erkenning van aanmeldingsdiensten voor digitale overheidstoepassingen die gebruik maken van niet-verbonden aanmeldingsmiddelen (hierna 'het ontwerp kb').

2. De Commissie brengt hierna dan ook bij hoogdringendheid advies uit over het ontwerp kb, rekening houdend met de informatie waarover zij beschikt.

II. HET WETTELIJK KADER

3. Het ontwerp kb geeft uitvoering aan de artikelen 133 tot 136 *van de programmawet van 8 april 2003* welke voorzien in een wettelijk kader voor het aanbieden van elektronische diensten aan de burgers via portalen of websites, en dit door het gebruik van een elektronische identificatie en authenticatie van de burger.

4. Het ontwerp kb geeft tevens uitvoering aan *de wet van 15 augustus 2012 houdende oprichting en organisatie van een federale dienstenintegrator* die de federale overheidsdienst informatie –en communicatietechnologie (Fedict) erkent als dienstenintegrator voor de federale overheid. In artikel 4, 3° van deze wet wordt bepaald dat Fedict instaat voor het bevorderen en het waken over de homogeniteit van de toegangsrechten tot de gegevensbanken. Overeenkomstig artikel 4, 4° van deze wet zorgt Fedict tevens voor het uitwerken van de technische modaliteiten om de toegangskanalen zo efficiënt en veilig mogelijk uit te bouwen.

III. ONDERZOEK VAN DE AANVRAAG

A. Context van de aanvraag

5. Overeenkomstig het verslag aan de Koning kadert het ontwerp kb in het globale e-governmentbeleid van de regering. Het toenemend gebruik van tablets en smartphones stelt de overheid voor de uitdaging om het groeiend aanbod van digitale overheidstoepassingen eveneens open te stellen voor deze nieuwe toestellen. Tevens wordt er gezocht naar oplossingen om aanmeldingen aan de hand van de elektronische identiteitskaart eenvoudiger te maken voor gebruikers. Nu gebeurt dit vaak aan de hand van een verbonden kaartlezer, maar veel burgers

beschikken niet over een dergelijk apparaat en het gebruik ervan wordt door velen als hinderlijk beschouwd omwille van de noodzakelijke software die moet worden geïnstalleerd.

6. Het ontwerp kb wil dan ook een kader scheppen waarbinnen een aanbieder van aanmeldingsdiensten voor niet-overheidstoepassingen door middel van een niet-verbonden aanmeldingsmiddel een erkenning kan bekomen om het aangeboden niet-verbonden aanmeldingsmiddel ook ter beschikking te stellen voor het gebruik voor digitale overheidstoepassingen. Een voorbeeld betreft de niet-verbonden aanmeldingsmiddelen voor thuisbankieren welke ook zouden kunnen worden gebruikt voor het lezen van elektronische identiteitskaarten in het kader van digitale overheidstoepassingen.

B. Algemeen standpunt van de Commissie

7. De Commissie stelt vast dat het ontwerp kb meerdere bepalingen bevat waarin reeds in detail geregeld wordt op welke manier de identificatie en authenticatie van burgers dient gerealiseerd te worden, in het bijzonder in bijlage II '*functionele en technische specificaties van de aanmeldingsdienst*'.

8. Artikel 16 WVP, stelt dat een verantwoordelijke voor de verwerking gepaste technische en organisatorische maatregelen dient te nemen. Deze maatregelen dienen een passend beveiligingsniveau te waarborgen. Om te bepalen welk beveiligingsniveau passend of geschikt is, voorziet de wet in vier criteria: de mogelijkheden of de stand van de techniek, de kosten voor de toepassing van de maatregelen, de aard van de te beveiligen gegevens en de potentiële risico's. Deze criteria impliceren onder andere dat de verantwoordelijke voor de verwerking zich steeds moet informeren over de diverse technieken die er op de markt zijn om gegevens en de verwerking ervan te beveiligen. Hij moet immers nagaan of dat wat ooit passend was, wel passend blijft[1].

9. Vanuit die optiek pleit de Commissie voor een aanpak die toelaat om ten allen tijde, en op een flexibele wijze, de (technische) beveiligingsmaatregelen te kunnen bijsturen. Wanneer deze in detail in de regelgeving zijn vastgelegd – zoals wordt voorgesteld in het ontwerp kb – vergt elke aanpassing van de maatregelen noodzakelijkerwijze ook een wijziging van het ontwerp kb, wat impliceert dat telkens een zware, tijdrovende procedure moet doorlopen worden. Dit gebrek aan flexibiliteit kan er in onderhavig geval toe leiden dat artikel 16 WVP in de praktijk dode letter blijft, omdat de kans bestaat dat niet (tijdig genoeg) wordt ingespeeld op nieuwe technologische ontwikkelingen. Om voornoemd risico te beperken, adviseert de Commissie om in het ontwerp kb minder in detail te treden en om er met name louter de functionaliteiten in te voorzien waaraan het

[1] D. De Bot, *Verwerking van persoonsgegevens*, Antwerpen, Kluwer, 2001, p. 253.

beoogde systeem dient te voldoen. De bijlage II met de concrete technische specificaties en beveiligingsmaatregelen dient derhalve niet te worden opgenomen in het ontwerp kb. Het ontwerp kb dient wel te voorzien dat de vaststelling en de validatie van de concrete technische specificaties en beveiligingsmaatregelen kan worden overgelaten aan het bevoegde sectorale Comité, met name het Sectoraal Comité van het Rijksregister. Fedict kan hiertoe een dossier indienen bij dit Comité. Deze methode zou een stuk flexibeler zijn en biedt in dit geval aldus ook meer garanties qua bescherming van persoonsgegevens.

C. Artikelsgewijze bespreking

Hiernavolgend worden enkel de voor de toepassing van de WVP relevante artikelen van het ontwerp kb geanalyseerd.

10. *Artikel 1* lijst de verschillende definities op. De definitie van 'niet-verbonden aanmeldingsmiddel' en 'verbonden aanmeldingsmiddel' is niet geheel duidelijk : is het onderscheid tussen beiden gebaseerd op draad versus draadloos ? Volgens de toelichting vanwege de aanvrager gaat het inderdaad om verbonden en niet-verbonden (draadloze) kaartlezers. Het verdient aanbeveling om dit te verduidelijken.

11. *Artikel 5* voorziet dat het niet-verbonden aanmeldingsmiddel bij verificatie van de elektronische identiteitskaart gebruik maakt van de cryptografische operaties met betrekking tot het identiteitscertificaat van de elektronische identiteitskaart. Hier kan de aanvrager verwijzen naar de relevante wettelijke bepalingen met betrekking tot de elektronische identiteitskaart. Desgevallend kunnen deze worden opgenomen in Bijlage II aan het ontwerp kb.

12. Overeenkomstig *artikel 7* moet een gebruiker zich voorafgaandelijk aanmelden bij de federale overheid om de aanmeldingsdienst te selecteren waarvoor hij zich wenst te registreren. Vervolgens moet de gebruiker zich ook éénmalig registreren bij de dienstverlener. Het is niet duidelijk welke data er worden geregistreerd bij de dienstverlener. Volgens de toelichting verstrekt door de aanvrager betreft het de noodzakelijke data om een controle van het identiteitscertificaat te kunnen doen : het serienummer en de uitgever van het identiteitscertificaat. De Commissie herinnert de aanvrager eraan dat, indien er persoonsgegevens zouden worden verwerkt door de dienstverlener, overeenkomstig artikel 4, §1, 3° WVP deze persoonsgegevens toereikend, terzake dienend en niet overmatig dienen te zijn, uitgaande van de doeleinden waarvoor zij worden verkregen of waarvoor zij verder worden verwerkt.

13. De registratie van de gebruiker is overeenkomstig *artikel 8* enkel mogelijk indien op het moment van de registratie het identiteitscertificaat van de elektronische identiteitskaart niet vervallen is, niet

herroepen is, en is uitgegeven door een erkende, niet-herroepen certificatieautoriteit. Deze voorwaarden zijn werkelijk noodzakelijk om de veiligheid van de dienst te verzekeren overeenkomstig artikel 16 WVP, bijvoorbeeld in het geval van een diefstal van een elektronische identiteitskaart met de bijbehorende pincode, waarbij Docstop werd verwittigd, en er dient over te worden gewaakt dat deze voorwaarden door de dienstverlener zorgvuldig worden gerespecteerd.

14. *Artikel 11* bepaalt dat de aanmeldingsdienst de erkennende overheid bij elke aanmelding de unieke identificatiecode van de gebruiker stuurt, op basis waarvan de erkennende overheid de identiteit van de gebruiker vaststelt. Het is niet duidelijk uit welke data deze unieke identificatiecode bestaat. Daarnaast dient te worden opgemerkt dat indien deze unieke identificatiecode gebruik zou maken van het identificatienummer van het Rijksregister, de dienstverlener voor dit gebruik gemachtigd dient te zijn of te worden gemachtigd door het Sectoraal Comité van het Rijksregister. Volgens de toelichting verstrekt door de aanvrager zou het om een willekeurige identificatiecode gaan.

15. Overeenkomstig *artikel 12* garandeert de dienstverlener dat het gebruik van het niet-verbonden aanmeldingsmiddel enkel mogelijk is indien op het moment van de aanmelding het identiteitscertificaat van de elektronische identiteitskaart niet vervallen is, niet herroepen is, en is uitgegeven door een erkende, niet-herroepen certificatieautoriteit. Zoals reeds gesteld onder randnummer 13, is dit een cruciale voorwaarde voor de veiligheid van de dienstverlening overeenkomstig artikel 16 WVP. De dienstverlener moet dan ook onmiddellijk over alle relevante informatie kunnen beschikken, bijvoorbeeld vanwege Docstop.

16. Overeenkomstig *artikel 15 §1* neemt de dienstverlener geen kennis van de digitale overheidstoepassingen waartoe de gebruiker door middel van zijn aanmeldingsdienst toegang verzoekt. Dit wordt herhaald in artikel 22 van Bijlage II aan het ontwerp kb. Dit is een belangrijke bepaling in het ontwerp kb, en maakt eveneens een toepassing uit van artikel 4, §1, 3° WVP. Het is belangrijk dat de dienstverlener geen kennis heeft van de door de gebruiker geconsulteerde e-gov toepassing, de dienstverlener dient voor de in het ontwerp kb beoogde doeleinden namelijk niet over deze informatie te beschikken. Dit zou daarenboven bij de dienstverlener een verwerking van gevoelige gegevens (bijvoorbeeld consultatie e-Health platform) kunnen uitmaken overeenkomstig de WVP, welke aan bijzondere bepalingen is onderworpen.

17. *Artikel 15, §2* voorziet dat de dienstverlener een beveiligd controlespoor installeert zodat de gegevens per specifieke transactie kunnen worden gereconstrueerd. Hiertoe bewaart de dienstverlener voor iedere aanmelding gedurende een termijn van 10 jaar de identiteit van de gebruiker, de aanmeldingsdienst waarmee de gebruiker zich aanmeldt en het tijdstip van aanmelding. Het is niet duidelijk wat onder 'de identiteit van de gebruiker' dient te worden

begrepen. Is hier bijvoorbeeld ook sprake van een verwerking van het identificatienummer van het Rijksregister ? Dit dient dan ook te worden verduidelijkt, en in overeenstemming te zijn met het proportionaliteitsbeginsel overeenkomstig artikel 4, §1, 3° WVP. Volgens de toelichting verstrekt door de aanvrager zou het enkel om de naam van de gebruiker gaan, hetgeen als proportioneel kan worden beschouwd. De keuze voor de bewaartermijn van 10 jaar, welke zou kunnen zijn ingegeven door bepaalde strafrechtelijke verjaringstermijnen, kan eveneens worden verduidelijkt in het verslag aan de Koning.

18. In *artikel 5 van Bijlage II* aan het ontwerp kb wordt onder punt 2 de 'minimale informatie' vermeld welke door de dienstverlener moet worden opgeslagen teneinde de geldigheid van de elektronische identiteitskaart te kunnen valideren op het moment van aanmelding. Volgens de toelichting verstrekt door de aanvrager betreft het de noodzakelijke data om een controle van het identiteitscertificaat te kunnen doen : het serienummer en de uitgever van het identiteitscertificaat.

19. In *artikel 6 van Bijlage II* aan het ontwerp kb is sprake van een unieke identificatiecode. De Commissie verwijst hieromtrent eveneens naar haar opmerkingen onder randnummer 14.

OM DIE REDENEN,

brengt de Commissie een **gunstig** advies uit over de huidige inhoud van het ontwerp kb op voorwaarde dat rekening wordt gehouden met de opmerkingen onder punten 9, 14, 16-17 van het voorliggende advies.

De Wnd. Administrateur, De Voorzitter,

(get.) Patrick Van Wouwe (get.) Willem Debeuckelaere