Aanbeveling nr 03/2009 van 1 juli 2009

Betreft: aanbeveling uit eigen beweging in verband met integratoren in de overheidssector (A/2007/043)

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 31;

Gelet op de adviezen nrs 01/2008 en 41/2008 die de Commissie uitbracht m.b.t. respectievelijk het ontwerp van decreet betreffende het elektronische bestuurlijke gegevensverkeer en het voorontwerp van wet houdende oprichting en organisatie van een Federale Dienstenintegrator;

Gelet op het verslag van de Voorzitter;

Brengt op 1 juli 2009 de volgende aanbeveling uit:

I. VOORWERP VAN DE AANBEVELING

1. Integratie is een generieke term. Gebruikt in verband met de verwerking van persoonsgegevens, kan deze term uiteenlopende ladingen dekken waarvan de gevolgen voor de persoonlijke levenssfeer sterk variëren.

2. Zo onderkent de Commissie de volgende vormen van integratie:

- de persoonsgegevensintegratie: het samenbrengen van persoonsgegevens uit verschillende authentieke bronnen en de opslag ervan in een aparte geïntegreerde gegevensbank, met het oog op de mededeling ervan aan derden;

- de dienstenintegratie: het afstemmen van elektronische deeldiensten op elkaar tot een coherent elektronisch dienstenpakket met het oog op de aanbieding ervan aan derden;

- de infrastructuurintegratie: het louter gebruiken van een gezamenlijke infrastructuur voor verwerkingen van persoonsgegevens zonder enige vorm van persoonsgegevensintegratie of dienstenintegratie (bijvoorbeeld gezamenlijk gebruik van servers, lijnen, solftware);

- de presentatie-integratie: louter geïntegreerd toegankelijk maken van persoonsgegevens of diensten via één elektronisch contactpunt, zonder enige vorm van persoonsgegevens- of dienstenintegratie (bijvoorbeeld een portaal, groene telefoon).

3. Deze aanbeveling handelt over de dienstenintegratie en de persoonsgegevensintegratie (hierna gegevensintegratie), in de overheidssector. Hun impact op de verwerking van persoonsgegevens is immers potentieel het meest privacybedreigend.

4. Hierna zullen deze vormen van integratie getoetst worden aan de principes van de WVP - eerlijkheid, rechtmatigheid en doelbinding, proportionaliteit, juistheid en nauwkeurigheid, transparantie, veiligheid, rechten van de betrokkene, aangifteplicht - met het oog op het vaststellen van een aantal vuistregels die daarbij in acht moeten worden genomen. In elk geval wordt verwacht dat instanties die in de overheidssector belast zijn met diensten- of persoonsgegevensintegratie steeds beschikken over een uitdrukkelijke wettelijke regeling terzake die voldoet aan de bepalingen van deze aanbeveling.

II. DIENSTENINTEGRATIE OF GEGEVENSINTEGRATIE?

5. Wanneer er zich m.b.t. de verwerking van persoonsgegevens verschillende alternatieven aanbieden met een gelijkwaardig efficiëntie- en effectiviteitsniveau, dan moet geopteerd worden voor datgene dat het minst bedreigend is voor de persoonlijke levenssfeer.

6. Indien het voor het verrichten van bepaalde taken noodzakelijk is dat men over gegevens afkomstig uit verschillende bronnen beschikt, dan vormt het ter beschikking stellen van deze gegevens door middel van dienstenintegratie meestal een minder privacybedreigende optie dan door middel van persoonsgegevensintegratie.

7. Bij dienstenintegratie worden de gegevens enkel tijdelijk samengebracht, namelijk op het ogenblik van het aanbod van de geïntegreerde dienst (concreet: op het ogenblik dat men de dienst interpelleert m.b.t. een bepaalde persoon of groep van personen). Dergelijke dienstverlening vereist niet het permanent samenbrengen van gegevens, noch de geïntegreerde opslag op langere termijn ervan. Doorgaans worden de gegevens rechtstreeks betrokken uit verschillende, betrouwbare gegevensbanken onder de verantwoordelijkheid van een welbepaalde entiteit, zgn. authentieke bronnen.

8. Een ontegensprekelijk voordeel van dergelijke werkwijze bestaat erin dat de onnodige circulatie wordt vermeden van kopieën van gegevensbestanden waarin persoonsgegevens zijn opgenomen die niet of niet regelmatig worden bijgewerkt en bijgevolg achterhaalde informatie - dus fouten - bevatten wat in het licht van artikel 4, § 1, 4°, WVP moet vermeden worden. Het vermindert bovendien het risico op onrechtmatige toegang tot de persoonsgegevens doordat de persoonsgegevens niet onnodig op verschillende plaatsen gedupliceerd worden.

9. De aanbieder van dienstenintegratie zal vaak optreden als een "trusted third party" (hierna TTP). Een TTP is *"an entity trusted by multiple other entities within a specific context and which is alien to their internal relationship*[1]*".* Een TTP is dus een vertrouwde onafhankelijke partij die diensten aanbiedt die de betrouwbaarheid van de elektronische gegevensuitwisseling en gegevensopslag vergroten en zelf geen opdracht of belang heeft inzake de eigenlijke inhoudelijke verwerking van de geïntegreerde persoonsgegevens. Haar reden van bestaan moet het tijdelijk samenbrengen van gegevens ten behoeve van derden zijn waarbij zij erover waakt dat zowel de WVP als de eventuele machtigingen van de bevoegde Sectorale comités geëerbiedigd worden. Bijvoorbeeld wanneer een machtiging voorschrijft dat aan de gemachtigde alleen een resultaat mag meegedeeld worden -

[1] blz. 16 van Consultation paper dd 23/11/2005 on "Common Terminological Framework for Interoperable Electronic Identity Management"

zoals inkomen hoger of lager dan een bepaald bedrag – maar niet de gegevens op zich, dan zal de TTP zorgen voor de eventuele berekening en het resultaat doorgeven.

10. Bij gegevensintegratie wordt een nieuwe gegevensbank gecreëerd waarin permanent informatie afkomstig uit verschillende bronnen wordt samengebracht en bewaard. Het betreft dus een concentratie van informatie op één plaats. Niettegenstaande dit in het licht van het doeleinde waarvoor deze gegevens werden samengebracht kan verantwoord zijn, kan men er niet omheen dat een veiligheidsincident i.v.m. dergelijke gegevensbank een veel zwaardere weerslag heeft op de persoonlijke levenssfeer dan een incident m.b.t. tot één van de bronnen waaruit de gegevens werden aangeleverd.

11. Vanuit WVP-oogmerk is dienstenintegratie dan ook te verkiezen boven gegevensintegratie. Dit laatste is slechts aanvaardbaar indien dit nodig is **en** de gewenste functionaliteit niet met een gelijkwaardige efficiëntie en effectiviteit kan gerealiseerd worden door middel van dienstenintegratie. Concreet betekent dit dat gegevensintegratie slechts geoorloofd is voor zover de verantwoordelijke voor de verwerking beschikt over hetzij een wettelijke basis, hetzij een gerechtvaardigd belang dat redelijkerwijze niet met een gelijkwaardige efficiëntie en effectiviteit kan behartigd worden via dienstenintegratie. "Redelijkerwijze" veronderstelt dat een afweging gemaakt wordt met oog voor alle facetten van het proces: wat is er nodig, wie heeft wat, wat kan geleverd worden en onder welke vorm, wat is technisch mogelijk, welke zijn de veiligheidsrisico's, wat zijn de budgettaire implicaties, …. dus eigenlijk een toetsing aan o.a. de artikelen 4, 5 en 16, § 4, WVP.

12. Het feit dat dienstenintegratie op een bepaald ogenblik geen optie is en dus tot gegevensintegratie wordt overgegaan, sluit niet uit dat dienstenintegratie op een bepaald ogenblik wel een haalbare kaart wordt en de werkwijze dienovereenkomstig moet worden aangepast. In het licht hiervan is het dan ook aangewezen dat in geval van gegevensintegratie periodiek geëvalueerd wordt of deze nog verantwoord is gelet op de evolutie van de onderliggende parameters.

III. CIRKELS VAN VERTROUWEN

13. Zoals hierboven reeds werd aangegeven, moet men erover waken dat er geen onnodige bedreigingen voor de bescherming van de persoonlijke levenssfeer ontstaan door het onnodig samenbrengen of dupliceren van persoonsgegevens.

14. Door beroep te doen op een gecoördineerd en modulair systeem van gebruikers-, toegangs- en loggingbeheer met gedecentraliseerde gegevensopslag waardoor verschillende partijen kunnen profiteren van elkaars elektronische toegangsbeheersmodules, authentieke bronnen en loggingsystemen, kan dit principe maximaal worden verzekerd voor wat de raadpleging van

gegevensbanken betreft. Het maakt komaf met meervoudige identieke controles en opslag van loggings.

15. Dergelijk samenwerkingsverband wordt vaak omschreven als "cirkels van vertrouwen". Deze worden gerealiseerd via een taakverdeling tussen de betrokken instanties waarbij duidelijke afspraken worden gemaakt over:

- wie welke authenticaties, verificaties en controles verricht aan de hand van welke middelen en daarvoor verantwoordelijk en aansprakelijk is;

- hoe tussen de betrokken instanties de resultaten van de verrichte authenticaties, verificaties en controles op een veilige wijze elektronisch worden uitgewisseld;

- wie welke loggings bijhoudt;

- hoe ervoor wordt gezorgd dat bij onderzoek, op eigen initiatief van een controleorgaan of n.a.v. klacht, volledig kan gereconstrueerd worden welke natuurlijke persoon welke dienst of transactie m.b.t. welke burger of onderneming wanneer, via welk kanaal en voor welke doeleinden heeft gebruikt.

IV. DIENSTENINTEGRATIE EN DE WVP

4.1. Eerlijkheid, rechtmatigheid en doelbinding

16. De Commissie wijst erop dat de verwerking van gegevens door dienstenintegratie in de overheidssector enkel toegestaan is wanneer ze geschiedt in één of meerdere gevallen vervat in artikel 5, eerste lid WVP.

17. Werken via een dienstenintegrator kan een positieve weerslag hebben op de bescherming van de persoonlijke levenssfeer. Indien deze dienstverlening goed georganiseerd is, is er in hoofde van de gebruikers weinig of geen ruimte om eventueel misbruik te maken van bijvoorbeeld de machtiging waarbij hen toegang verleend wordt tot een authentieke gegevensbron. Het werken met verwijzingsrepertoria (zie punt 25) kan helpen om ongeoorloofde raadplegingen te vermijden.

18. Gelet op zijn impact moet de dienstenintegratie beschouwd worden als een afzonderlijk doeleinde en niet zomaar de afgeleide van of inherent aan een ander doeleinde. De finaliteit "dienstenintegratie" is immers de maatstaf aan de hand waarvan alle aspecten van dit integratieproces moeten worden beoordeeld op ondermeer hun doelgebondenheid, hun

proportionaliteit, hun veiligheid. Deze toetsing vereist dat het doeleinde "dienstenintegratie" duidelijk wordt omschreven en afgebakend (welbepaald). Het domein dat de dienstenintegrator bestrijkt vormt hierbij een niet te verwaarlozen factor. Wanneer bijvoorbeeld gevoelige gegevens (artikelen 6 tot 9) worden versast, zal moeten worden nagegaan of de specifieke randvoorwaarden daartoe vervuld zijn.

19. De meerwaarde van de dienstenintegratie wordt afgemeten aan de diensten die hij overspant zodat ze niet elk afzonderlijk moeten aangesproken worden. Men moet dus weten welke diensten ingekapseld worden zoals bijvoorbeeld de toegang tot welke authentieke gegevensbron, tot welke soort transacties, …. Een duidelijke communicatie dienaangaande door de dienstenintegrator is dus onontbeerlijk.

20. Daarnaast veronderstelt het aanbieden van de geïntegreerde dienst dat de verschillende deelprocessen op elkaar worden afgestemd. Het coördineren (= orkestreren) ervan impliceert het maken van precieze afspraken over het uitvoeren van de diverse taken zoals bijvoorbeeld toegestane verwerkingstijd van een aanvraag, het tijdig doorgeven van statusinformatie, enz. Deze afspraken vinden hun neerslag in de *service level agreements* die de dienstenintegrator dienaangaande afsluit. Dit zijn overeenkomsten tussen de aanbieder(s) en de afnemer(s) van bepaalde diensten waarin de te leveren diensten en hun kwaliteitsniveau evenals de rechten en plichten van beiden dienaangaande worden bepaald.

21. Voor de burger zal dienstenintegratie niet altijd een doorzichtig gebeuren zijn. Het is dus primordiaal dat de dienstenintegrator duidelijk opgeeft wie de verantwoordelijke van de verwerking is, waar men zijn recht van toegang, verbetering en wissing kan uitoefenen (meer details in afdeling 4.6., randnummers 41 e.v.). Er moet te allen prijze vermeden worden dat de burger wordt ontmoedigd om zijn rechten uit te oefenen omdat het voor hem onmogelijk is om het (de) juiste aanspreekpunt(en) te identificeren.

4.2. Proportionaliteit

22. Het werkterrein van een dienstenintegrator moet duidelijk afgelijnd en voldoende homogeen zijn zodat een potentiële gebruiker voor een specifiek domein over een duidelijk aanspreekpunt beschikt en een eenduidige toepassing van veiligheids- en privacybeschermende normen en maatregelen wordt gewaarborgd (zie ook randnummer 34).

23. Dienstenintegratie is erop gericht om niet meer of niet langer persoonsgegevens op te slaan dan nodig voor de levering van geïntegreerde diensten of voor andere doeleinden die daarmee verband houden, bijvoorbeeld de reconstructie van een transactie ingeval van een klacht. Dit

principe is van toepassing zowel op de verstrekte persoonsgegevens als op de persoonsgegevens die nodig zijn om dit te kunnen doen.

24. Concreet betekent dit dat er beroep wordt gedaan op een reeks van authentieke bronnen die voor de gebruiker op een gebruiksvriendelijke wijze met elkaar in verband worden gebracht zodat gelijkwaardige voordelen worden bekomen van een geïntegreerde gegevensopslag zonder dat die effectief plaatsvindt.

25. Dienstenintegratie kan soms nuttig worden ondersteund door het beheer van een verwijzingsrepertorium. Dergelijk repertorium kan de basis vormen voor de organisatie van de elektronische gegevensuitwisseling en kan bestaan uit onderling gerelateerde tabellen, waaronder:

- een tabel van beschikbare diensten en informatie waarin wordt vermeld welke diensten of informatie bij een actor beschikbaar is m.b.t. de verschillende soorten dossiers (de wat-waar-tabel);

- een tabel van toegangsgerechtigde gebruikers en toepassingen, die een lijst bevat van de gebruikers en toepassingen aan wie toegang mag verleend worden maar ook de authenticatie-instrumenten en –regels en de toegangsprofielen[2] (de wie-krijgt-wat-tabel);

- een personenrepertorium dat aangeeft welke personen in welke hoedanigheid dossiers bezitten bij welke actoren m.b.t. welke periodes (de wie-waar-hoe-wanneer-tabel);

- een inschrijvingstabel waarin wordt vermeld welke gebruikers en toepassingen in welke gevallen en voor welke personen in welke hoedanigheid welke automatische diensten wensen te bekomen.

26. Dit verwijzingsrepertorium kan worden opgebouwd rekening houdende met de in punt 15 vermelde principes van de cirkels van vertrouwen, zodat bepaalde onderdelen kunnen worden gedecentraliseerd, in het bijzonder wanneer uit de erin vermelde gegevens informatie kan worden afgeleid die bijzonder wordt beschermd door of krachtens de WVP.

27. De dienstenintegrator mag enkel persoonsgegevens verwerken die relevant en niet overmatig zijn voor de gebruikers van de geïntegreerde dienst (toepassing van artikel 4 WVP). Dit betekent dat:

---

[2] In het toegangsprofiel wordt vastgelegd op welke soort van informatie of dienst een beroep kan gedaan worden en gedurende welke periode afhankelijk van de hoedanigheid waarin een persoon of onderneming geregistreerd is.

- er aan de gebruikers geen gegevens mogen worden doorgestuurd waarop deze geen recht hebben rekening houdend zowel met de modaliteiten van de eventuele machtigingen als met de doeleinden;

- de dienstenintegrator zelf slechts die persoonsgegevens mag verzamelen die noodzakelijk zijn om de gebruikers hun informatie te kunnen bezorgen en een volledige audit te verrichten.

28. De dienstenintegrator moet bij de dienstenintegratie de eventuele machtigingen naleven, waardoor aan een gebruiker toegang wordt verleend tot persoonsgegevens. In een machtiging worden zowel de doeleinden bepaald waarvoor zij wordt verleend evenals de gegevens waartoe de gemachtigde mag toegang hebben. Zij kan ook nog andere modaliteiten bevatten:

> *Bijvoorbeeld*: het kan voor een gebruiker relevant zijn om te weten of het inkomen van een persoon al of niet hoger is dan een bepaald bedrag. Het exacte bedrag hoeft hij echter niet te kennen om zijn doeleinden te kunnen realiseren. In dat geval zal de machtiging doorgaans bepalen dat hem alleen maar een ja/neen antwoord mag verstrekt worden. De dienstenintegrator zal ervoor moeten zorgen dat alleen het antwoord aan de gebruiker wordt bezorgt, niet de onderliggende gegevens.

29. Het miskennen van machtigingen stelt zowel de dienstenintegrator als de gebruiker bloot aan sancties (artikel 39 WVP). De dienstenintegrator moet dus maatregelen treffen om zoiets te voorkomen. Indien een machtiging werd afgeleverd, weet de dienstenintegrator duidelijk wat er moet gegarandeerd worden. Dit is minder evident wanneer er bij derden gegevens kunnen opgevraagd worden waarvoor geen machtigingsvereiste geldt. In dat geval zal de dienstenintegrator moeten verifiëren of de gevraagde gegevens relevant en niet overmatig zijn met het oog op het doeleinde waarvoor een gebruiker op zijn diensten beroep doet. De afwezigheid van een machtiging ontslaat de dienstenintegrator niet van de naleving van de artikelen van de WVP.

4.3. Juistheid en nauwkeurigheid

30. Door middel van de dienstenintegratie worden aan de gebruiker ervan een aantal gegevens ter beschikking gesteld, doorgaans na voorafgaande toetsing van het doeleinde (welbepaald, welomschreven en gerechtvaardigd) en de proportionaliteit van de gegevens door een sectoraal of vergelijkbaar comité.

31. Op basis van deze gegevens treft die gebruiker beslissingen of onderneemt hij acties jegens welbepaalde personen. Hierbij is het zowel voor de gebruiker als voor de betrokkenen belangrijk dat de gegevens op basis waarvan wordt gehandeld, juist zijn. Foute gegevens kunnen ertoe leiden dat een betrokkene bijvoorbeeld een recht miskend ziet terwijl de gebruiker van zijn kant geconfronteerd wordt met vermijdbare betwistingen van zijn beslissingen (kosten, extra werk).

32. Nu rust in toepassing van artikel 4, § 1, 4°, WVP, sowieso op iedere verantwoordelijke voor de verwerking de verplichting om ervoor te zorgen dat de verwerkte gegevens nauwkeurig zijn. De dienstenintegrator moet systemen uitbouwen waarbij de kennisgeving van het feit dat een bepaald gegeven onjuist is, onmiddellijk wordt doorgegeven aan de leverancier van het gegeven opdat deze onmiddellijk het nodige zou kunnen doen om dit te verbeteren. Dit neemt niet weg dat het aanbeveling verdient dat de dienstenintegrator dienaangaande voorafgaandelijk duidelijke afspraken maakt met de leveranciers van de deeldiensten in een *service level agreement*. Naar de gebruikers toe heeft dit het voordeel dat zij precies kunnen worden geïnformeerd over de kwaliteit van de geleverde gegevens en diensten zodat zij een inschatting kunnen maken van de gevolgen van de dienstenintegratie op hun werkzaamheden.

4.4. Transparantie

33. Het verdient aanbeveling dat de dienstenintegrator duidelijke informatie omtrent alle facetten van zijn werking openbaar maakt zodat eenieder de mogelijkheid heeft om de regelmatigheid van zijn optreden te verifiëren. Dit betekent in de eerste plaats dat hij het doel van de dienstenintegratie moet omschrijven en toelichten. Dit doeleinde is immers de maatstaf op basis waarvan wordt vastgesteld of zijn verwerking daadwerkelijk doelgebonden zijn. Dit houdt onder meer in dat hij duidelijk moet aanduiden welke diensten hij samenbrengt, welke verwerkingen hij erop uitvoert en volgens welke *service level agreements* hij werkt.

34. Het werkterrein van een dienstenintegrator moet eveneens duidelijk worden afgelijnd teneinde de overlapping van de actiedomeinen van dienstenintegratoren te vermijden. Dit is cruciaal omdat:

- het zowel voor de gebruikers als voor buitenstaanders moet duidelijk zijn via welke dienstenintegrator en volgens welke regels o.a. inzake veiligheid er moet gewerkt worden;

- aan "shopping" doen tussen de dienstenintegratoren moet uitgesloten zijn. Dergelijk fenomeen zou immers op termijn nefast zijn voor de informatieveiligheid. Om te kunnen besparen op de uitgaven voor bijvoorbeeld informatieveiligheid, zal een gebruiker geneigd zijn om in zee te gaan met de integrator die dienaangaande de minste eisen stelt. Gevolg: een nivellering van de veiligheid naar beneden toe in plaats van naar boven;

- er wordt uitgesloten dat dienstenintegratoren op hetzelfde terrein gelijktijdig en dus tot verwarring leidende initiatieven zouden ontwikkelen.

35. Door dienstenintegratie verkrijgt de gebruiker, mits de vereiste machtiging, toegang tot de persoonsgegevens – zonder tussenkomst van de betrokken burger - die hij nodig heeft om zijn taken uit te voeren. De burger mag echter niet gedegradeerd worden tot het lijdend voorwerp van deze evolutie. Om dit te vermijden verdient het aanbeveling dat de gebruiker aan de burger meldt op welke gegevens hij een beslissing of een actie steunt zodat de burger kan controleren of er met correcte gegevens werd gewerkt. Dit is een absolute must opdat deze laatste zijn recht van verbetering ten volle zou kunnen uitoefenen. In dit verband wordt ook aangestipt dat de machtigingen tot gegevensuitwisseling publiek zijn. Zij worden voor wat de Sectorale comités in de schoot van de Commissie betreft, op haar website bekendgemaakt zodat iedere burger kan controleren - wie gemachtigd is – waarom - welke gegevens - uit welke authentieke bronnen - te verkrijgen.

36. Hierbij aansluitend pleit de Commissie ervoor om ervoor te zorgen dat de burger een overzicht kan krijgen omtrent welke gegevens door wie zijn geraadpleegd door beroep te doen op een dienstenintegrator. Dit kan worden vormgegeven overeenkomstig de hogervermelde principes van de cirkels van vertrouwen. De wetenschap dat de burger, die het best geplaatst is om te detecteren wanneer zijn gegevens ten onrechte werden geraadpleegd, over dergelijke inzagerecht beschikt kan alleen maar het correct gebruik van de verleende machtigingen ten goede beïnvloeden.

37. Het kan tevens aanbevolen worden dat een dienstenintegrator wordt, daar waar mogelijk, medebeheerd door vertegenwoordigers van de datasubjecten. Een dienstenintegrator zal vooral oog hebben voor de behoeften van de gebruikers. De aansturing van de dienstenintegrator door een entiteit, die uit de aard van haar samenstelling oog heeft voor de belangen van de datasubjecten, waarborgt dat de belangen van deze laatsten niet uit het oog worden verloren.

4.5. Veiligheid

38. Het verzekeren van de veiligheid impliceert dat structurele, organisatorische, juridische, personele, technische en fysische maatregelen worden genomen zodat het risico op de miskenning van de WVP geminimaliseerd wordt. Deze maatregelen moeten er dus concreet voor zorgen dat de dienstenintegrator:

- garandeert redelijkerwijze dat de persoonsgegevens die verwerkt worden voor dienstenintegratie niet voor andere doeleinden worden verwerkt (artikel 4 WVP – zie ook afdeling 4.1);

- de integriteit, de authenticiteit, de beschikbaarheid en de vertrouwelijkheid van de persoonsgegevens die hij verwerkt redelijkerwijze waarborgt en hij daartoe afspraken maakt met de onderscheiden tussenkomende partijen in de hele dienstverleningsketen (*service level agreements*);

- de preventieve controle van de rechtmatigheid en proportionaliteit van de dienstenintegratie verzekert (artikel 4 WVP – zie ook punten 28-29);

- garandeert dat persoonsgegevens niet onrechtmatig kunnen gewijzigd of vernietigd worden tijdens de verwerking (artikel 16 WVP);

- de auditeerbaarheid (wie, wat, wanneer, over wie en waarvoor) van de verwerking van de persoonsgegevens over de hele dienstverleningsketen heen verzekert en daartoe afspraken maakt met de onderscheiden tussenkomende partijen in de hele dienstverleningsketen;

- niet exporteert naar derde landen zonder passend beschermingsniveau (artikel 21 WVP);

- de veiligheidsmaatregelen uitwerkt volgens het principe van de "cirkels van vertrouwen" (zie punten 13-15).

39. Het verdient aanbeveling dat de dienstenintegrator over een interne informatieveiligheidsdienst beschikt met een stimulerende, coördinerende en eventueel controlerende functie t.a.v. de aanbieders van deeldiensten en de gebruikers van geïntegreerde diensten. Dit ontslaat noch de aanbieders noch de gebruikers van de verplichting om over een eigen informatieveiligheidsbeleid en eventueel informatieveiligheidsdienst te beschikken. Deze diensten zullen immers de gesprekspartners bij uitstek zijn van de veiligheidsdienst van de dienstenintegrator. In onderling overleg zullen zij moeten nagaan hoe een maximale veiligheid kan verzekerd worden. In een eerste fase zal ervoor gezorgd worden dat alle participanten naar een aanvaardbaar veiligheidsniveau getild worden om die vervolgens stapsgewijze te verfijnen en dus de verbeteren. Hierbij kan ter inspiratie verwezen worden naar het referentiekader van de ISO-normenreeks 27000 (beveiligingseisen t.o.v. personeel, beheer van communicatie- en bedieningsprocessen, toegangsbeveiliging, ontwikkeling en onderhoud van systemen, continuïteitsmanagement, beveiligingsorganisatie, enz).

40. De naleving van de veiligheidsvereisten door de dienstenintegrator en gebruikers van geïntegreerde diensten zou jaarlijks kunnen worden geëvalueerd aan de hand van de invulling van een checklist m.b.t. minimale veiligheidsnormen goedgekeurd door een extern controleorgaan, bij voorkeur een Sectoraal comité van de Commissie of een vergelijkbaar machtigingsorgaan. Er zijn immers grenzen aan de eisen die een dienstenintegrator kan opleggen aan aanbieders van deeldiensten en de gebruikers van geïntegreerde diensten. De minimale veiligheidsnormen en de externe controle erop is dus een gepast instrument om een degelijke handhaving terzake te waarborgen. Het Comité zou het verder kunnen blijven genieten van een machtiging afhankelijk kunnen stellen van bijkomende inspanningen op veiligheidsgebied door een betrokkene.

4.6. Rechten van de betrokkene

41. Artikel 10 WVP verleent de burger het recht om inzage te krijgen van zijn gegevens vanwege de verantwoordelijke voor de verwerking. Wanneer de burger geconfronteerd wordt met de beslissing of een actie van een gebruiker van dienstenintegratie, is het voor de eerstgenoemde niet altijd vanzelfsprekend tot wie hij zich zal moeten richten om zijn gegevens in te kijken en dit recht daadwerkelijk te kunnen uitoefenen.

42. Het correct informeren van de burger houdt dus in dat de gebruiker van de dienstenintegratie niet alleen vermeldt op welke gegevens hij zich steunt, maar tevens wie de betrokken verantwoordelijken van de verwerking zijn. Dit laat de burger toe om enerzijds de betrouwbaarheid van de beslissing van de gebruiker te appreciëren en anderzijds weet hij tot welke verantwoordelijke van de verwerking hij zich moet richten.

43. Dit laatste is niet alleen van belang met het oog op het uitoefenen van het inzagerecht maar eveneens met het oog op het recht op kosteloze verbetering van onjuiste persoonsgegevens en/of de kosteloze verwijdering van persoonsgegevens *die gelet op het doel van de verwerking, onvolledig of niet ter zake dienend zijn, of waarvan de registratie, de mededeling of de bewaring verboden zijn, of die na verloop van de toegestane duur zijn bewaard* (artikel 12 WVP).

44. Hierbij kan aangestipt worden dat het recht op verbetering in hoofde van de burger, eigenlijk een meerwaarde oplevert voor de dienstenintegratie. Immers de verbetering van onjuiste gegevens komt uiteindelijk alle gebruikers van de dienstenintegratie ten goede.

V. GEGEVENSINTEGRATIE EN DE WVP

5.1. Eerlijkheid, rechtmatigheid en doelbinding

45. De Commissie wijst erop dat gegevensintegratie in de overheidssector enkel toegelaten is wanneer ze nuttig is voor of meerdere situaties vervat in artikel 5, eerste lid WVP **en**, zoals reeds werd aangegeven in punten 10 tot 12, de gewenste functionaliteit niet met eenzelfde efficiëntie en effectiviteit kan geleverd worden door middel van dienstenintegratie. Vanuit WVP-perspectief is gegevensintegratie slechts verantwoord indien een privacyvriendelijker alternatief, zoals dienstenintegratie, niet haalbaar is.

46. Gegevensintegratie is een afzonderlijk doeleinde en niet zomaar de afgeleide van of inherent aan een ander doeleinde. De finaliteit "gegevensintegratie" is immers de maatstaf aan de hand van dewelke alle aspecten van dit proces op hun conformiteit met de WVP worden beoordeeld (de doelgebondenheid, de proportionaliteit, de veiligheid, enz.). Deze toetsing vereist dat het doeleinde "gegevensintegratie" duidelijk wordt omschreven en afgebakend (welbepaald). Het domein dat gegevensintegrator bestrijkt vormt hierbij een niet te verwaarlozen factor. Wanneer bijvoorbeeld gevoelige gegevens (artikelen 6 tot 9) worden geïntegreerd, zal moeten worden nagegaan of de specifieke randvoorwaarden daartoe vervuld zijn.

47. De gegevens die geïntegreerd worden moeten duidelijk omschreven worden. Er kan geen vrede genomen worden met een vage en algemene aanduiding, zoniet is een ernstige toetsing van hun proportionaliteit uitgesloten met als voor de hand liggend risico dat niet pertinente gegevens worden opgenomen. Dit sluit trouwens aan bij het recht van iedere burger om te weten welke gegevens een bepaalde verantwoordelijke van de verwerking m.b.t. hem verwerkt (artikel 10 WVP).

48. De gegevensintegrator moet duidelijk opgeven wie de verantwoordelijke van de verwerking is bij dewelke een burger zijn recht van toegang, verbetering en wissing kan uitoefenen (zie afdeling 4.6.). Er moet ten alle prijzen vermeden worden dat de burger wordt ontmoedigd om zijn rechten uit te oefenen omdat het voor hem onmogelijk is om het juiste aanspreekpunt te identificeren.

49. De gegevens worden door de gegevensintegrator en verantwoordelijke van de verwerking samengebracht met het oog op een welbepaald doeleinde. De mate waarin dergelijke geïntegreerde gegevens aan een derde, een gebruiker, kunnen verstrekt worden hangt af van de mate waarin het doeleinde waarvoor deze laatste deze gegevens wenst, verenigbaar is met het doeleinde van de betrokken integrator. Die verenigbaarheid wordt beoordeeld rekening houdend met de redelijke verwachtingen of de reglementaire bepalingen ter zake (artikel 4, § 1, 2°, WVP).

5.2. Proportionaliteit

50. In bepaalde gevallen zal men genoodzaakt zijn over te gaan tot gegevensintegratie om een bepaalde taak uit te voeren of een doeleinde te realiseren, bijvoorbeeld het aanmaken van statistieken. Deze geïntegreerde gegevens moeten conform de WVP worden verwerkt. Dit betekent dat als het voor de realisatie van het doeleinde niet vereist dat een link kan gelegd worden met een welbepaalde fysieke persoon, alleen een opslag van deze gegevens onder anonieme of minstens gecodeerde vorm verantwoord is. Alleen wanneer het doeleinde vereist dat er kan worden teruggekoppeld naar een individu, mogen de geïntegreerde gegevens opgeslagen worden in een vorm waardoor zulks mogelijk is.

51. Deze principes zijn eveneens van toepassing op de verzending van geïntegreerde gegevens. Er moet voorrang gegeven worden aan een verzending onder anonieme of gecodeerde vorm. Een niet-gecodeerde verzending is slechts geoorloofd voor zover wordt aangetoond dat de gebruiker zijn doeleinde aan de hand van anonieme gegevens niet kan realiseren.

52. Een aantal principes die i.v.m. de proportionaliteitsproblematiek naar voor werden geschoven in het luik handelend over de dienstenintegratie, moeten bij analogie doorgetrokken worden naar de gegevensintegratie:

- de noodzaak om het toepassingsgebied van een gegevensintegrator duidelijk en voldoende homogeen af te bakenen;

- het beheer van loggings volgens het principe van de "cirkels van vertrouwen";

- er mogen enkel persoonsgegevens samengebracht worden die relevant en niet overmatig zijn voor de gebruikers van de geïntegreerde gegevens wat een toetsing aan het doeleinde van deze laatsten noodzakelijk maakt;

- hierbij aansluitend moeten er gepaste maatregelen getroffen worden opdat een gebruiker enkel gegevens krijgt m.b.t. personen waarvoor deze gegevens relevant en niet overmatig zijn in het licht van het door de betrokken gebruiker nagestreefde doeleinde;

- de naleving van de machtigingen verleend door een sectoraal comité van de Commissie of een vergelijkbaar orgaan;

5.3. Juistheid en nauwkeurigheid

53. Net zoals een dienstenintegrator verdient het aanbeveling dat een gegevensintegrator met de leveranciers van de gegevens die het voorwerp uitmaken van de integratie *service level agreements* afsluiten in verband met de juistheid en de nauwkeurigheid van de aangeleverde persoonsgegevens. De kwaliteit van de geïntegreerde gegevens wordt er immers door bepaald. Dit houdt bijvoorbeeld afspraken in met betrekking tot de timing waarbinnen wijzigingen of verbeteringen van gegevens door de verstrekkers moeten worden gesignaleerd aan de integrator. Achterhaalde gegevens halen immers de kwaliteit van de geïntegreerde gegevens naar beneden. Voor de gebruikers is dit trouwens pertinente informatie voor de inschatting van de weerslag ervan op hun werkzaamheden.

54. Nu mag de kwaliteit van de aangeleverde gegevens nog zo goed zijn, als hun integratie niet zorgvuldig gebeurt, is het resultaat en dus de juistheid van de geïntegreerde gegevens, ondermaats met alle gevolgen van dien voor de gebruikers. Bijvoorbeeld een gebruiker weigert ten onrechte een tegemoetkoming aan een burger omdat sommige geïntegreerde gegevens op iemand anders betrekking hebben. De gegevensintegrator moet dus maatregelen nemen om ervoor te zorgen dat de samengevoegde gegevens betrekking hebben op een en dezelfde persoon. De samenvoeging verrichten aan de hand van het identificatienummer van het Rijksregister zou bijvoorbeeld een van die maatregelen kunnen zijn.

5.4. Transparantie

55. Gelet op de privacyimpact van de gegevensintegratie moet een maximale transparantie worden verzekerd. Het verdient aanbeveling dat de gegevensintegrator duidelijke informatie omtrent alle facetten van zijn werking openbaar maakt zodat eenieder de mogelijkheid heeft om de regelmatigheid van zijn optreden te verifiëren.

56. Deze transparantie kan naast het verstrekken van openbare informatie ook worden bekomen door vertegenwoordigers van de datasubjecten te betrekken bij het beheer of de controle van de gegevensintegrator. De Commissie verwijst in dit verband naar de suggesties die over dit aspect in het hoofdstuk over de dienstenintegratie formuleerde en die hier kort in herinnering worden gebracht, namelijk er moet geïnformeerd worden over:

- het doel van de gegevensintegratie;
- het toepassingsgebied van de gegevensintegratie,
- de gebruikers van de geïntegreerde gegevens;
- de verantwoordelijke van de verwerking waarbij het recht van toegang, verbetering en wissing kan uitgeoefend worden.

5.5. Veiligheid en rechten van de betrokkene

57. De Commissie verwijst naar de vuistregels die ze in dit verband m.b.t. dienstenintegratie uitwerkte (zie randnummers 38 e.v.).

Voor de Administrateur m.v., De Voorzitter,

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