Aanbeveling nr 02/2010 van 31 maart 2010

Betreft: Aanbeveling omtrent de privacybeschermende rol van Trusted Third Parties (TTP) bij gegevensuitwisseling (A/09/022)

De Commissie voor de bescherming van de persoonlijke levenssfeer (hierna de Commissie);

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 30;

Gelet op het 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* (hierna het KB van 13 februari 2001);

Gelet op het verslag van de Voorzitter;

Brengt op 31 maart 2010 de volgende aanbeveling uit:

I. INLEIDING

1. "Trusted Third Party" (hierna "TTP"), ook wel genoemd "Third Trusted Party", "vertrouwde derde partij" of "vertrouwde tussenpersoon", is *"an entity trusted by multiple other entities within a specific context and which is alien to their internal relationship"*[1] [2].

2. De notie "TTP" wordt in vaak sterk verschillende contexten gebruikt. Ook de Commissie heeft al verschillende adviezen uitgebracht waarin sprake is van een "TTP". Meestal betroffen het zijdelingse opmerkingen naar aanleiding van specifieke dossiers. Onderhavige aanbeveling heeft tot doel om de TTP op een meer systematische en integrale manier te benaderen. De Commissie wenst hierbij in het bijzonder te onderzoeken in welke gevallen de tussenkomst van een dergelijke TTP een meerwaarde kan bieden op het vlak van de bescherming van de persoonlijke levenssfeer.

II. DE "TRUSTED THIRD PARTY" IN HET BELGISCH RECHT

3. "TTP" is een begrip dat vele ladingen dekt[3]. De Belgische wetgever heeft ervoor gekozen om een aantal specifieke TTP's wettelijk te regelen. De wet van 15 mei 2007 *tot vaststelling van een juridisch kader voor sommige verleners van vertrouwensdiensten* voorziet met name in regels voor de volgende TTP-functies[4]:

- dienst voor elektronische archivering
- dienst voor elektronische tijdsregistratie
- dienst voor elektronisch aangetekende zending
- dienst voor de tijdelijke blokkering van gestorte sommen

4. De Commissie erkent dat deze TTP's een meerwaarde kunnen bieden voor bepaalde punctuele aspecten van privacy-bescherming. De "dienst voor elektronische tijdsregistratie" zal bijvoorbeeld kunnen bijdragen tot de nauwkeurigheid van gegevens (cf. art. 4, § 1, 4°, WVP) en de "dienst voor elektronisch aangetekende zending" zou bij bepaalde gegevensverwerkingen als een onderdeel van de toepassing van artikel 16 WVP (veiligheid) kunnen beschouwd worden.

---

[1] blz. 16 van Consultation paper dd 23/11/2005 on *"Common Terminological Framework for Interoperable Electronic Identity Management"* (https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/GlossaryDoc#4_44_Trusted_third_party_TTP).

[2] Dit betreft slechts één van de mogelijke definities van het concept "TTP".

[3] Ter illustratie kan worden verwezen naar een Nederlandse studie, consulteerbaar via volgend link: http://www.cbpweb.nl/downloads_av/AV22.pdf?refer=true&theme=purple.

[4] Cf. J. Dumortier en G. Somers, "De wet van 15 mei 2007 tot vaststelling van een juridisch kader voor sommige verleners van vertrouwensdiensten: een eerste verkenning", *T.B.H.* 2007/7, p. 649-659.

5. Desalniettemin wordt op deze TTP-functies hier niet verder ingegaan. De Commissie wenst zich in onderhavige aanbeveling immers toe te spitsen op de gevallen waarin een TTP tussenkomt als schakel bij de uitwisseling van persoonsgegevens en waarbij deze interventie structureel is ingegeven vanuit privacy-beschermende overwegingen.

III. TRUSTED THIRD PARTIES ALS PRIVACY-BESCHERMERS BIJ DATA-UITWISSELING

6. De Commissie ziet zes gevallen waarbij de motieven voor de inschakeling van een "TTP" bij gegevensuitwisseling zich volledig op het vlak van privacy-bescherming situeren. Hierna worden deze gevallen systematisch uitgelegd.

A. TTP die gegevens anonimiseert

7. Een TTP kan instaan voor het anonimiseren van persoonsgegevens. Gelet op de definitie van "anonieme gegevens"[5], impliceert dit dat wanneer de TTP haar anonimiseringsopdracht heeft vervuld, de door hem verwerkte gegevens op geen enkele manier meer kunnen in verband worden gebracht met een natuurlijke persoon, ook niet door de TTP zelf.

B. TTP die gegevens codeert

8. Een TTP kan ook gegevens coderen. Een codering van persoonsgegevens moet worden gezien als een transformatie van de gegevens waardoor zij niet meer in verband kunnen worden gebracht met een of meerdere geïdentificeerde of identificeerbare personen en waarbij de aangewende transformatietechnieken niet gekend zijn door de uiteindelijke ontvanger van de gegevens.

9. De term "code" slaat aldus op de transformatiemechanismen en de eventuele parameters die voor de transformatie werden gebruikt. Ter illustratie kan op de volgende technieken worden gewezen:

- "randomisatie" van een gegeven: hier wordt een gegeven vervangen door een aselect of willekeurig gegeven (bijvoorbeeld het identificatienummer dat wordt vervangen door een volgnummer van dossieropmaak of door een getal dat toevalsgewijs wordt gegenereerd);
- permutatie van gegevens: hier worden twee gegevens van twee verschillende personen binnen eenzelfde categorie omgewisseld (bijvoorbeeld: geboortedatum van twee personen

[5] *"anonieme gegevens" : gegevens die niet met een geïdentificeerd of identificeerbaar persoon in verband kunnen worden gebracht en derhalve geen persoonsgegevens zijn* (artikel 1, 5°, KB van 13 februari 2001).

geboren in hetzelfde decennium wordt omgewisseld). De permutatie kan ook worden doorgevoerd tussen meer dan twee individuen;

- berekeningsalgoritme: hier wordt een gegeven vervangen door een ander gegeven dat op het eerste gegeven werd berekend (bijvoorbeeld in stukken hakken of vervanging van het identificatienummer door een al dan niet omkeerbare hashcode);
- versluiering van gegevens: hier worden de gegevens vervangen door andere gegevens met behulp van een logisch of mathematisch algoritme en die gegevens worden verkregen door op een of meerdere gegevens van meerdere gevallen uit de steekproef verrichtingen uit te voeren.

C. TTP die gegevens aggregeert

10. Bij het aggregeren van gegevens, worden deze data in groepen verenigd waardoor het (quasi) onmogelijk wordt om op basis van de door de TTP geleverde resultaten individuele personen te identificeren.

11. Ter illustratie: stel dat een onderzoeker wil weten hoeveel nieuwe gevallen van longkanker er in 2008 werden vastgesteld en bij welke leeftijdscategorie deze diagnose het meeste werd gesteld. In een dergelijk geval heeft de onderzoeker geen gedetailleerde persoonsgegevens nodig. Het volstaat dat hij een getal krijgt van het totale aantal gevallen per leeftijd. Een tussenkomst van een TTP kan dit resultaat opleveren. Geaggregeerde gegevens zeggen dus iets over de resultaten op niveaus 'boven' de individuele diagnoses.

D. TTP die (mede) instaat voor toegangscontrole

12. De Commissie heeft al verschillende keren gesteld – onder andere in advies nr. 30/98 van 25 september 1998– dat leden van beroepen waarvoor er een orde of een instantie met disciplinaire bevoegdheid bestaat, slechts toegang tot het Rijksregister zouden mogen hebben indien deze instantie als tussenpersoon optreedt. Personen die toegang wensen zouden aan deze laatste de reden van de raadpleging kunnen meedelen – wat controle van de finaliteit van de raadpleging mogelijk maakt – en de desbetreffende instantie zou ook kunnen nagaan of die persoon bijvoorbeeld geen tuchtstraf heeft gekregen (iets wat de beheerder van een authentieke bron doorgaans niet kan onderzoeken). De TTP treedt dan aldus op als een eerste filter tegen misbruik.

13. Een dergelijke aanpak kan het gebruikers –en toegangsbeheer van authentieke bronnen aanzienlijk verbeteren[6]. De orde (of een andere instantie met disciplinaire bevoegdheid) – die

[6] Zie in dit verband ook aanbeveling nr. 01/2008 van 24 september 2008.

optreedt als een TTP – fungeert als bewaker voor het rechtmatig gebruik door haar leden van een authentieke bron zoals het Rijksregister. Zij staat garant voor het feit dat diegene die een authentieke bron raadpleegt ook effectief in functie is en zij waakt bovendien ook over de doelgebondenheid van de raadplegingen. Op die wijze kan met andere woorden een autocontrole door de sector zelf georganiseerd worden.

14. De Commissie wijst in deze context ook op de taken van de integratoren zoals bedoeld in haar aanbeveling nr. 03/2009 van 1 juli 2009, daar zij eveneens een belangrijke rol kunnen spelen bij de organisatie van het gebruikers –en toegangsbeheer van authentieke bronnen, zij het wel op een andere manier dan ordes (of andere instanties met disciplinaire bevoegdheid)[7].

E. TTP die bijstand verleent bij de verzending van documenten zonder de bekendmaking van de identiteit van de betrokkenen

15. Ter illustratie kan worden verwezen naar de rol van het Rijksregister in het kader van contactname voor reunies, herdenkingen, familieresearch, waarvan sprake in aanbeveling nr 02/2009 van 27 mei 2009. In voornoemde aanbeveling wordt ten aanzien van de diensten van het Rijksregister gesuggereerd om – onder bepaalde modaliteiten – hun medewerking te verlenen aan de lokalisatie van personen om sociale of humanitaire redenen, meer bepaald door het doorsturen van de brieven van een aanvrager zonder dat hem het adres van de bestemmeling wordt meegedeeld. De aanvrager bereikt hierbij zijn doel, namelijk zijn boodschap bereikt de bestemmeling en tegelijk wordt de privacy van de bestemmeling gerespecteerd. Deze laatste beslist immers zelf of hij contact opneemt met de aanvrager en desgevallend zijn actuele adres meedeelt.

16. Een ander voorbeeld betreft de intermediaire rol van het Rijksregister bij de doorgifte van schriftelijke surveys aan mensen uit een steekproef[8]. Indien het gaat om schriftelijke vragenlijsten[9]

---

[7] Ter illustratie kan worden verwezen naar beraadslaging nr. 36/2006 van 20 december 2006 en beraadslaging nr. 08/031 van 3 juni 2008, waarbij CORVE respectievelijk door de Commissie voor de Bescherming van de Persoonlijke Levenssfeer *loco* het sectoraal comité van het Rijksregister en door het Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid Afdeling « Sociale Zekerheid », werd gemachtigd om toegang te hebben tot persoonsgegevens afkomstig uit het Rijksregister van de natuurlijke personen en de Kruispuntbankregisters van de KSZ, om aldus haar taak als doorgeefluik van de betrokken persoonsgegevens ten behoeve van de Vlaamse doeltoepassingen te kunnen vervullen. Elke opzoeking die door een Vlaamse doeltoepassing wordt verricht, wordt door CORVE gelogd. Het is CORVE die de toegang tot de persoonsgegevens controleert en er zorg voor zal dragen dat de persoonsgegevens afkomstig van het Rijksregister van de natuurlijke personen en de Kruispuntbankregisters uitsluitend verder worden meegedeeld aan de respectieve bevoegde afdelingen van de Vlaamse overheid, overeenkomstig de geldende machtigingen bepaald door of krachtens de wet dan wel bij beslissing van het bevoegde sectoraal comité van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer. Zowel de Commissie zelf als het Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid waren dergelijke werkwijze genegen daar ze de garantie op een correcte uitvoering van de machtigingsbeslissingen verhoogt.

[8] Cf. advies uit eigen beweging nr. 27/2008 van 3 september 2008 en het identieke addendum bij het vademecum *"privacy en onderzoek"* dat de Commissie uitbracht in oktober 2008 (eerste druk).

voor een eenmalige bevraging zal het Rijksregister met name zelf de verzending van de vragenlijsten met introductiebrieven verzorgen, weliswaar op basis van materiaal dat wordt aangebracht door de onderzoeksinstelling. Ook de nazendingen kunnen op dezelfde wijze worden bezorgd. Het Rijksregister maakt in dit geval enkel in gecodeerde vorm die informatie over aan de onderzoeksinstelling die nodig is om een analyse van de non-respons mogelijk te maken.

IV. VOORWAARDEN WAARAAN TTP's DIENEN TE VOLDOEN

A. Voorwaarden waaraan alle TTP's die worden vermeld in titel III van deze aanbeveling dienen te voldoen

17. De Commissie adviseert dat alle TTP's die het voorwerp uitmaken van onderhavige aanbeveling de volgende principes zouden respecteren:

- de TTP moet – samen met de andere betrokken verantwoordelijke(n) voor de (latere) verwerking – in het algemeen waken over de correcte naleving van de wetgeving inzake de persoonlijke levenssfeer.
  Dit impliceert ook dat wanneer een TTP vaststelt dat de gegevensverwerkingen waarin hij tussenkomt op bepaalde punten niet conform de WVP dreigen te verlopen, het aangewezen is dat hij hier de verantwoordelijke(n) voor de (latere) verwerking op wijst, ook al betreft het aspecten van de verwerking waarvoor hijzelf juridisch niet (geheel) verantwoordelijk is. De Commissie denkt hierbij in het bijzonder aan de naleving van het finaliteits –en proportionaliteitsbeginsel en aan het respecteren van de aangifteplicht en/of machtigingsverplichting(en);

- de TTP mag de gegevens die hij heeft verwerkt in het kader van zijn TTP-functie(s) niet voor andere doeleinden gebruiken dan de specifieke doelen waarmee hij werd belast;

- een TTP dient de gepaste technische en organisatorische maatregelen te treffen die nodig zijn voor de bescherming van de persoonsgegevens tegen toevallige of ongeoorloofde vernietiging, tegen toevallig verlies, evenals tegen de wijziging van of de toegang tot, en iedere andere niet toegelaten verwerking van persoonsgegevens. Concreet heeft dit ondermeer de volgende implicaties:

---

[9] Een schriftelijke enquête vormt de regel en de mondelinge enquête de uitzondering. Indien de onderzoeker niet kan of wil werken met een schriftelijke vragenlijst wordt dat aangevraagd en gemotiveerd bij het Sectoraal Comité van het Rijksregister.

- een TTP mag enkel speciaal door haar aangeduide personen toegang verlenen tot de gegevens die het voorwerp uitmaken van koppeling en die personen dienen door de TTP aan een vertrouwelijkheidsplicht te worden onderworpen. Zij mogen de gegevens enkel raadplegen indien dit nodig is opdat de TTP haar opdracht zou kunnen vervullen.
  Een TTP moet ook een lijst opstellen van deze personen die zij op eventueel verzoek van de Commissie moet kunnen voorleggen, zeker indien de gegevens die aan verwerking worden onderworpen deze zijn waarvan sprake in de artikelen 6 t.e.m. 8 WVP (cf. artikel 25 KB van 13 februari 2001);

- de TTP dient bij voorkeur, al dan niet onder zijn personeel, een consulent inzake informatieveiligheid en bescherming van de persoonlijke levenssfeer aan te wijzen;

- een TTP dient zich te organiseren volgens de cirkels van vertrouwen[10];

➢ de verwerkingen die door een TTP worden uitgevoerd dienen transparant te verlopen. Dit impliceert ondermeer dat:

- de verantwoordelijken van de oorspronkelijke en/of van de latere verwerking, vanwege de TTP minstens de volgende informatie moeten verkrijgen:
  - de werking van de TTP en de voorwaarden voor het gebruik van de diensten van de TTP;
  - de draagwijdte van de aansprakelijkheid van de TTP.
- de betrokkenen – op basis van de door de TTP en de verantwoordelijken voor de oorspronkelijke en/of latere verwerking verstrekte informatie – steeds moeten kunnen weten bij wie zij hun recht van toegang, verbetering, verwijdering of niet-aanwending kunnen uitoefenen.

B. <u>Bijkomende voorwaarden voor TTP's die gegevens anonimiseren (cf. titel III, punt A, van onderhavige aanbeveling)</u>

18. Naast de hoger uiteengezette algemene voorwaarden (cf. supra randnummer 17), dient een TTP die gegevens anonimiseert ook specifiek rekening te houden met de volgende richtsnoeren:

➢ een TTP moet de persoonsgegevens vernietigen die hem door de verantwoordelijken van de oorspronkelijke verwerking werden bezorgd, zodra hij zijn anonimiseringsopdracht heeft

[10] Cf. aanbeveling nr. 03/2009, randnummers 13-15.

vervuld, tenzij het een opdracht betreft waaruit voorvloeit dat hij de gegevens moet bewaren;

- een TTP moet alle technische middelen aanwenden om een mogelijke identificatie van de betrokken personen door de verantwoordelijke voor de (latere) verwerking onmogelijk te maken.

C. Bijkomende voorwaarden voor TTP's die gegevens coderen (cf. titel III, punt B van onderhavige aanbeveling)

i. TTP die gegevens codeert en die optreedt als "intermediaire organisatie" in de zin van hoofdstuk II van het KB van 13 februari 2001

19. "TTP" wordt vaak als een synoniem gebruikt voor de term "intermediaire organisatie" (hierna "IO") in de zin van artikel 1, 6°, van het KB van 13 februari 2001[11]. Er zijn een aantal waarborgen in datzelfde hoofdstuk II van het KB opgenomen[12]. Het betreft meer bepaald de volgende regels:

- een IO dient voldoende onafhankelijk te zijn ten overstaan van de verantwoordelijke voor de latere verwerking (de ontvanger van de gecodeerde data)[13].
  Deze onafhankelijkheid kan volgens de Commissie op verschillende manieren worden bereikt. Dit kan evident door de functie van IO te laten uitoefenen door een instantie die geen enkele band heeft met de gegevensverwerking waarin de TTP tussenkomt.
  Een andere mogelijkheid betreft het geval waarin de IO wordt beheerd of aangestuurd door een groep van gebruikers. Het feit dat één van deze gebruikers in concrete gevallen een belang kan hebben legt niet noodzakelijk een hypotheek op de onafhankelijkheid van de IO, aangezien het gezamenlijke gewicht van de andere gebruikers in dergelijke situaties de onafhankelijkheid kan waarborgen;

---

[11] Ter illustratie, zie: K. Van Gossum en G. Verhenneman, "De informatisering van de kankerregistratie in België", *Computerrecht* 2008, p. 281.

[12] De Commissie wijst er op dat de term "intermediaire organisatie" in hoofdstuk II van dit KB van 13 februari 2001 beperkter dient te worden geïnterpreteerd dan de notie "TTP". De rol van een IO is beperkt tot het coderen van persoonsgegevens in het kader van latere verwerkingen voor historische, statistische of wetenschappelijke doeleinden (hierna "HSW-doeleinden") die op zich niet verenigbaar zijn met de doeleinden van de oorspronkelijke gegevensinzameling. De IO staat hierbij enkel in voor het omzetten van niet-gecodeerde persoonsgegevens naar gecodeerde gegevens, ten behoeve van een verantwoordelijke voor de latere verwerking met "HSW-doeleinden". Een "TTP" kan daarentegen bijvoorbeeld optreden buiten de context van een latere verwerking (zie ook infra randnummers 30 e.v.).

[13] Artikel 11 van het KB van 13 februari 2001.

- een IO moet de gepaste technische en organisatorische maatregelen nemen om te beletten dat gecodeerde gegevens in niet-gecodeerde worden omgezet[14];

- een IO kan gecodeerde gegevens slechts meedelen met het oog op de latere verwerking ervan voor historische, statistische of wetenschappelijke doeleinden tegen overlegging door de verantwoordelijke voor de latere verwerking van het ontvangbewijs van een volledige aangifte bij de Commissie[15];

- de verantwoordelijke voor de oorspronkelijke verwerking van persoonsgegevens of de IO moeten voorafgaand aan de codering van gevoelige, gerechtelijke of gezondheidsgegevens (artikelen 6-8 WVP) bepaalde informatie aan de betrokkenen mededelen[16], tenzij
  - deze verplichting onmogelijk blijkt of onevenredig veel moeite kost[17] of
  - de IO een administratieve overheid betreft die door of krachtens de wet de uitdrukkelijke opdracht heeft om persoonsgegevens samen te brengen en te coderen, en hierbij onderworpen is aan door of krachtens de wet vastgelegde specifieke maatregelen die de bescherming van de persoonlijke levenssfeer tot doel hebben[18].

  De verantwoordelijke voor de oorspronkelijke verwerking of de IO die dergelijke gegevens wenst te coderen zonder voorafgaande kennisgeving aan de betrokken persoon, vult de aangifte bij de Commissie aan met welbepaalde informatie, waarna de Commissie een aanbeveling geeft[19].

20. De Commissie adviseert ook dat TTP's die gegevens coderen en die optreden als IO – naast de hoger door de Commissie beschreven algemene richtsnoeren (cf. supra randnummer 17) – alle technische middelen zouden aanwenden om een mogelijke identificatie van de betrokken personen door de verantwoordelijke voor de (latere) verwerking onmogelijk te maken. Concreet impliceert dit onder andere:

- dat in een bijzondere beveiliging moet worden voorzien van de methoden en/of parameters gebruikt bij de codering;

- dat de TTP er steeds over moet waken dat de ter beschikking gestelde gecodeerde gegevens niet dermate gedetailleerd zijn dat heridentificatie mogelijk wordt. Een dergelijke

[14] Artikel 12 van het KB van 13 februari 2001.

[15] Artikel 13 van het KB van 13 februari 2001.

[16] Artikel 14 van het KB van 13 februari 2001.

[17] Artikel 15, eerste lid, van het KB van 13 februari 2001.

[18] Artikel 15, tweede lid, van het KB van 13 februari 2001.

[19] Artikel 16 van het KB van 13 februari 2001.

heridentificatie kan immers mogelijk zijn door de door de TTP verstrekte gegevens aan mekaar te linken of door deze te linken aan informatie waarover de ontvanger reeds beschikt.

21. De Commissie neemt ook de gelegenheid te baat om een aantal stellingen die soms worden ingenomen inzake de tussenkomst van een IO te bevestigen of integendeel, te ontkrachten. Het betreft meer bepaald de volgende stellingen:

a. een IO moet ook steeds onafhankelijk zijn van de gegevens*leverancier(s);*
b. de tussenkomst van een IO is enkel nodig wanneer gegevens van de verschillende gegevensleveranciers betrekking hebben op dezelfde natuurlijke personen.

22. De stelling in punt a. is te verregaand. Artikel 11 van het KB van 13 februari 2001 legt immers enkel een onafhankelijkheidsplicht op voor de IO ten overstaan van de verantwoordelijke voor de latere verwerking (de ontvanger van de gecodeerde data). Indien een IO optreedt als verwerker van de verantwoordelijke voor de oorspronkelijke verwerking, werkt hij trouwens onder diens controle, toezicht en instructie conform artikel 16 WVP en kan er dus van onafhankelijkheid geen sprake zijn. In termen van de WVP is een verwerker geen derde ten opzichte van de verantwoordelijke voor de verwerking (zie art. 1, § 6 WVP). Vanuit die invalshoek bekeken is de IO in de zin van het KB niet altijd onafhankelijke schakel ten opzichte van zowel de zendende (verantwoordelijke voor de oorspronkelijke verwerking) als de ontvangende zijde (verantwoordelijke voor de latere verwerking).

23. Inzake de stelling in punt b.[20] is het inderdaad correct dat artikel 10 van het KB van 13 februari 2001 – althans in een letterlijke interpretatie ervan – geen onderscheid maakt tussen het geval waarin de gegevens van de verschillende leveranciers betrekking hebben op verschillende dan wel op dezelfde natuurlijke personen.

24. De Commissie is evenwel van oordeel dat de interpretatie die stelt dat artikel 10 van het KB van 13 februari 2001 ook de situatie viseert waarbij de verantwoordelijke voor de latere verwerking persoonsgegevens wil inzamelen bij verschillende entiteiten over verschillende betrokkenen, geen

[20] Zie Vandendriessche, J.: "de verwerking van persoonsgegevens voor historische, statistische en wetenschappelijke doeleinden", *Tijdschrift voor Belgisch burgerlijk recht*, 2006, p. 541 en 543: *"Deze verplichte tussenkomst (van een IO, nvdr) wordt in het Verslag aan de Koning gerechtvaardigd door het bijzondere gevaar voor de persoonlijke levenssfeer die zou voortvloeien uit de samenvoeging van verschillende gegevensbestanden. Dit argument overtuigt maar gedeeltelijk. Er bestaat ongetwijfeld een gevaar indien de verantwoordelijke voor de verwerking bij verschillende andere entiteiten persoonsgegevens zal inzamelen over dezelfde betrokkenen. Op die manier ontstaat immers een "rijker" bestand. De redenering gaat echter niet helemaal op indien de verantwoordelijke voor de verwerking persoonsgegevens over verschillende betrokkenen inzamelt bij verschillende entiteiten. De aard van het gegevensbestand wijzigt er niet door. Er ontstaat enkel een groter gegevensbestand".*

rekening houdt met de concrete bedoeling van de verplichte tussenkomst van een IO. Deze verplichting verklaart zich namelijk vanuit het risico dat de gegevens over dezelfde betrokkenen, afkomstig van verschillende aangevers, zullen worden samengebracht om aldaar aan elkaar te worden gelinkt en gekoppeld. Hierdoor beschikt de IO immers over meer gegevens van de betrokkene dan elke gegevensleverancier. Een dergelijk "verrijkt" bestand laat hen ook toe om eventuele verbanden tussen de diverse persoonsgegevens te leggen.

Dit risico is echter niet voorhanden indien de verantwoordelijke voor de latere verwerking persoonsgegevens over verschillende betrokkenen wil inzamelen bij meerdere entiteiten. Bovendien zou deze visie met zich brengen dat de samenvoeging van twee kleine bestanden met persoonsgegevens op die manier strenger wordt beoordeeld dan de communicatie van een veel grotere, maar voor het overige identieke, databank door één verantwoordelijke voor de verwerking[21]. De Commissie gaat er dus van uit dat artikel 10 van het koninklijk besluit van 13 februari 2001 enkel de specifieke situatie beoogt waarin de verantwoordelijke voor de latere verwerking persoonsgegevens over dezelfde betrokkenen wil inzamelen bij verschillende entiteiten. Enkel dan worden gegevens immers gekoppeld waardoor nieuwe, (verrijkte) gegevens betreffende die persoon ontstaan.

ii. TTP die gegevens codeert en die optreedt buiten de context van hoofdstuk II van het KB van 13 februari 2001

25. De tussenkomst van een TTP is ook denkbaar voor het coderen van gegevens buiten de context van latere verwerking voor HSW-doeleinden. Hierbij kan worden verwezen naar de gevallen waarin de gegevens oorspronkelijk reeds voor onderzoeksdoeleinden werden verzameld of situaties waarin de TTP optreedt in het kader van een latere verwerking die verenigbaar is met het oorspronkelijk doeleinde.

26. In deze gevallen is hoofdstuk II van het KB van 13 februari 2001 niet van toepassing. De bijzondere eisen van dit hoofdstuk II slaan immers slechts op situaties waarin men een latere verwerking voor HSW-doeleinden wenst uit te voeren die op zich onverenigbaar is met het doeleinde waarvoor de gegevens oorspronkelijk werden verwerkt. Indien de latere verwerking voor HSW-doeleinden daarentegen verenigbaar is met het oorspronkelijke doeleinde, bv. omdat zij wordt toegestaan of opgelegd door een wettelijke of reglementaire bepaling[22], moeten de bijkomende

---

[21] Zie Vandendriessche, J., *o.c.*, p. 543.

[22] Deze vaststelling vloeit voort uit de interpretatie van artikel 4, § 1, 2° lid van de WVP. Dit artikel stelt dat *"persoonsgegevens dienen … niet verder te worden verwerkt op een wijze die, rekening houdend met alle relevante factoren, met name … met de toepasselijke wettelijke en reglementaire bepalingen, onverenigbaar is met die doeleinden."* De Commissie leidde hieruit af dat een verwerking, op basis van wettelijke of reglementaire bepalingen kan beschouwd worden als een toelaatbare en verenigbare verwerking, waarop de bepalingen met betrekking tot de latere verwerking vastgelegd in het uitvoeringsbesluit van de WVP niet van toepassing zijn (zie in die zin tevens bv. advies nr. 14/2002 van 8 april 2002). Zie ook het Verslag aan de

garanties waarvan sprake in Hoofdstuk II van het KB van 13 februari 2001 in principe niet worden gerespecteerd[23], aangezien het doelbindingsprincipe gevrijwaard blijft en de bedreiging voor een schending van de persoonlijke levenssfeer dus per definitie kleiner is.

27. De verenigbaarheid van een latere verwerking met de oorspronkelijke finaliteit doet evenwel geen afbreuk aan de overige verplichtingen onder de WVP en de andere hoofdstukken van het KB van 13 februari 2001:

- zo kan de logica die in hoofdstuk II van het KB 13 februari 2001 wordt gevolgd met betrekking tot de verplichting om de verwerking van anonieme of gecodeerde gegevens te verkiezen boven de verwerking van ongecodeerde gegevens[24], ook in deze gevallen aangewend worden, door toepassing te maken van het proportionaliteitsbeginsel (artikel 4, § 1, 3° WVP), dat vereist dat men niet meer gegevens mag verwerken (in casu mededelen) dan nodig voor de vooropgestelde doelstellingen (en waaruit kan worden afgeleid dat ook hun graad van identificatie niet overmatig mag zijn);

- de tussenkomst van een TTP is weliswaar niet steeds verplicht, maar is in het licht van artikel 16, § 4, WVP toch aanbevolen wanneer gegevens – over dezelfde betrokkenen – dienen gecodeerd te worden die uit verschillende bronnen afkomstig zijn;

- ook dient een gegevensverwerking steeds eerlijk (artikel 4, § 1, 1° WVP) en goed beveiligd (artikel 16, § 4, WVP) te verlopen . Vanuit die optiek dringt de Commissie er op aan om in voorkomend geval minstens in organisatorische maatregelen te voorzien opdat de codering van gegevens – die uit verschillende bronnen afkomstig zijn en die betrekking hebben op dezelfde betrokkenen – zou gebeuren door een eenheid die afgescheiden is van de dienst die het onderzoek uitvoert;

Koning bij het KB (p 7847): *"Een verenigbaar doeleinde is dus een doeleinde (….) dat op grond van een wetsbepaling als verenigbaar wordt beschouwd".* Een verdere verwerking voor HSW-doeleinden als gevolg van wettelijke of reglementaire bepalingen is dus op zich conform met artikel 4 § 1, 2°, eerste zin van de WVP. De bijzondere eisen van hoofdstuk II KB slaan dus slechts op de gevallen waar men beroep wenst te doen op artikel 4 § 1, 2°, tweede zin, van de WVP (de 'niet-onverenigbaarheid' van HSW-finaliteiten) om een verwerking op te zetten die anders niet zou mogen.

[23] Zie letterlijk het Verslag aan de Koning bij het KB (p 7847).: *"Wanneer persoonsgegevens oorspronkelijk worden verzameld voor historische, statistische of wetenschappelijke doeleinden of hergebruik van die gegevens met dat doel niet onverenigbaar is met het oorspronkelijk doeleinde, is ongeacht of al dan niet voldoende waarborgen voorhanden zijn, de gewone regeling voor verwerkingen van persoonsgegevens van toepassing*".

[24] Artikel 1 van het koninklijk besluit van 13 februari 2001, waarin definities zijn vastgelegd van de noties *"gecodeerde gegevens"* en *"niet-gecodeerde-gegevens"* is overigens onverkort van toepassing in deze situaties.

- de specifieke informatieverstrekking die wordt voorzien voor de latere verwerking van gevoelige, gerechtelijke en gezondheidsgegevens[25] geldt in deze context niet, maar anderzijds dient wel te worden voldaan aan artikel 26 van het KB van 13 februari 2001, op grond waarvan vooraf de redenen van die verwerking aan de betrokkenen moeten worden medegedeeld, alsmede de lijst van de categorieën van personen die toegang hebben tot deze gegevens.

28. Het feit dat hoofdstuk II van het KB van 13 februari 2001 in deze niet van toepassing is, heeft in de praktijk dus eerder beperkte gevolgen, daar de TTP *de facto* aan heel wat verplichtingen uit voornoemd hoofdstuk dient te voldoen. Op het vlak van de aangifte van de gegevensverwerking bij de Commissie zijn er evenwel significante verschillen:

- er hoeft geen aangifte voor een *latere* verwerking te gebeuren;
- het volstaat dat een gewone aangifte wordt verricht, die desgevallend – wanneer gevoelige of gerechtelijke gegevens worden verwerkt – wordt aangevuld met de informatie bedoeld in artikel 25, 4° van het KB van 13 februari 2001[26].

29. Verder wijst de Commissie in deze context nog op dezelfde aandachtspunten zoals supra in randnummer 20 uiteengezet (die evident gelden naast de algemene voorwaarden die in titel IV van onderhavige aanbeveling werden toegelicht).

iii. Slotbemerking: aanbeveling van de Commissie inzake de wenselijkheid van de tussenkomst van een TTP bij het coderen van gegevens

30. Hoger werd er reeds op gewezen dat de tussenkomst van een IO slechts in een aantal gevallen verplicht is krachtens het KB van 13 februari 2001. Deze redenering werd doorgetrokken naar TTP's die gegevens coderen maar die geen IO zijn in de zin van het KB (cf. randnummer 27, tweede pijltje). Een belangrijk criterium om te bepalen of de tussenkomst van een TTP verplicht/aangewezen is betreft dus of er gegevens – over dezelfde betrokkenen – worden samengebracht uit verschillende bronnen dan wel of er slechts één bron is.
De Commissie wenst hieraan evenwel nog één richtsnoer toe te voegen: in situaties waarin gegevens achteraf nog moeten kunnen gedecodeerd worden; beveelt zij aan dat de codering – ongeacht of de gegevens uit één of meerdere bronnen aangeleverd worden – gebeurt door een TTP (IO) en niet door de oorspronkelijke gegevensbron(nen). Een tussenkomst van een TTP biedt in dergelijke situaties immers extra waarborgen om ongeoorloofde decoderingen te vermijden.

---

[25] Artikel 14 e.v. van het KB van 13 februari 2001 (cf. supra randnummer 19).

[26] *"hij moet in de kennisgeving die krachtens artikel 9 van de wet aan de betrokken persoon moet worden gedaan of in de aangifte bedoeld in artikel 17, § 1, van de wet melding maken van de wet of verordening op grond waarvan de verwerking van persoonsgegevens bedoeld in de artikelen 6 tot 8 van de wet is toegestaan.*

D. <u>Bijkomende voorwaarden voor TTP's die gegevens aggregeren (cf. titel III, punt C, van onderhavige aanbeveling)</u>

31. De TTP moet alle technische middelen aanwenden om een identificatie van de betrokken personen door de verantwoordelijke voor de (latere) verwerking onmogelijk te maken. Hij moet de persoonsgegevens dus op een voldoende hoog niveau aggregeren. De Commissie meent bjivoorbeeld dat de door de TTP meegedeelde resultaten in principe geen groepen mogenbevatten die minder dan drie elementen bevatten.

32. Ter illustratie: stel dat de TTP, in het voorbeeld dat hoger werd gegeven (cf. supra randnummer 11), vaststelt dat er in 2008 maar bij één persoon van 21 jaar longkanker werd vastgesteld, dan moet er worden naar gestreefd om dit resultaat op een hoger aggregatieniveau aan de onderzoeker mee te delen, door bijvoorbeeld enkel te melden dat er in de leeftijdscategorie tussen 20 en 25 jaar tien gevallen werden vastgesteld. Het mededelen van resultaten voor de exacte leeftijd van 21 jaar, zou in dit geval immers belangrijke risico's op heridentificatie met zich meebrengen.

V. IS EEN TTP VERWERKER OF VERANTWOORDELIJKE VOOR DE VERWERKING ?

33. De vraag of de TTP optreedt als verantwoordelijke voor de verwerking dan wel als verwerker in de zin van de WVP, wordt voor de gevallen bedoeld in Hoofdstuk II, van het KB van 13 februari 2001 (IO), expliciet in voornoemd KB vermeld (met name, hetzij als verwerker van de enige gegevensverstrekker, hetzij als verantwoordelijke voor de verwerking bij meerdere gegevensverstrekkers), terwijl dit vraagstuk in alle andere in titel III van onderhavige aanbeveling vermelde situaties niet altijd met zekerheid kan worden gesteld. Ter zake geeft de Commissie de volgende richtsnoeren mee:

- wanneer persoonsgegevens van dezelfde betrokkenen bij verschillende gegevensverstrekkers worden opgevraagd en door de TTP worden samengebracht alvorens te worden gekoppeld, ontstaat een bijzondere bedreiging voor de bescherming van de persoonlijke levenssfeer. Dit vereist dan ook dat een TTP passende waarborgen biedt.

  Vandaar dat de Commissie van oordeel is dat in dergelijke gevallen de TTP niet kan optreden als loutere verwerker, maar autonoom moet kunnen worden aangesproken als afzonderlijke verantwoordelijke voor de verwerking en dit specifiek voor de verwerkingen die hij uitvoert;

- ook in andere situaties zal de TTP vaak als verantwoordelijke voor de verwerking kunnen worden gekwalificeerd. Dit zal met name het geval zijn indien de TTP één van de weinige spelers op de markt is die een bijzondere dienst kan leveren en indien de netwerkstructuur die hij installeert met zich meebrengt dat de gegevensverwerking noodzakelijkerwijze op een welbepaalde manier wordt verricht (zonder dat de verantwoordelijken voor de oorspronkelijke en de latere verwerkingen ter zake inspraak hebben). Ter illustratie kan hierbij worden gedacht aan de Kruispuntbank van de Sociale Zekerheid;

- de Commissie wijst er tot slot op dat wanneer het doel en de middelen van de uitgevoerde gegevensverwerkingen regelgevend omkaderd is, de verantwoordelijke voor de verwerking door de regelgever dient te worden aangeduid (artikel 1, § 4, WVP).

VI. TTP's EN INTEGRATOREN IN DE OVERHEIDSSECTOR

34. De Commissie brengt haar aanbeveling inzake integratoren in de overheidssector in herinnering. Zij is er zich van bewust dat de rol van een TTP en van een integrator in de overheidssector soms zullen samenvallen.

35. Zij ziet de verhouding tussen beide concepten als volgt: diensten –en gegevensintegratoren in de overheidssector zullen – indien zij aan de voorwaarden uit aanbeveling nr 03/2009 van 1 juli 2009 voldoen - ook als TTP kunnen optreden.[27] Zij zullen in principe – binnen hun eigen bevoegdheidssfeer – de rol kunnen vervullen van alle TTP-functies die worden opgesomd in titel III.

36. Het omgekeerde geldt echter niet: een TTP zal niet altijd een integrator in de zin van aanbeveling nr. 03/2009 zijn. Een essentieel verschil tussen beide betreft immers dat TTP's niet altijd bij of krachtens de wet moeten worden gemachtigd om hun rol te kunnen vervullen. Voor dienstenintegratie binnen de overheidssector is een dergelijke wettelijk mandaat echter wel onontbeerlijk. Er moet inderdaad vastgesteld worden dat de bestaande dienstenintegratoren[28] allen zijn (of zullen worden) ingebed in een strikt wettelijk of decretaal kader.

37. Alle TTP-functies die worden opgesomd in titel III kunnen dus in principe ook worden uitgeoefend door private instellingen, inzonderheid dan deze vermeld onder punten A tot en met C. Hierbij gelden evenwel belangrijke beperkingen voor wat betreft gegevens die aan of door

---

[27] In aanbeveling nr. 03/2009 (randnummer 34) heeft de Commissie er de nadruk op gelegd dat het werkterrein van een dienstenintegrator duidelijk moet worden afgelijnd teneinde de overlapping van de actiedomeinen van dienstenintegratoren te vermijden.

[28] Bv. Kruispuntbank van de Sociale Zekerheid, eHealth-platform, Fedict.

overheidsinstanties worden medegedeeld. TTP's die vandaag tussenkomen in overheidssectoren waar de gegevensuitwisseling door een bijzondere wetgeving wordt gereglementeerd zijn bv. allen openbare instellingen. Ter illustratie kan worden gewezen op artikel 14 van de wet van 15 januari 1990 houdende *oprichting en organisatie van de Kruispuntbank van de sociale zekerheid*, op grond waarvan elke mededeling van sociale gegevens van persoonlijke aard door of aan instellingen van sociale zekerheid, in principe via de Kruispuntbank van de sociale zekerheid dient te verlopen. Het is dan ook ondenkbaar dat in dit domein de TTP-functie door een private onderneming zou worden uitgeoefend[29].

VII. SLOTBEMERKING : DRAAGWIJDTE VAN ONDERHAVIGE AANBEVELING

38. Hoger werd aangegeven dat de Commissie erkent dat in een aantal gevallen de tussenkomst van een TTP een meerwaarde kan betekenen om de persoonlijke levenssfeer van betrokkenen te beschermen bij gegevensuitwisselingen. Zij geeft hierbij een aantal richtsnoeren, alsook bepaalde indicaties omtrent de wijze waarop zij bepaalde regels uit het KB van 13 februari 2001 interpreteert.

39. Zij is er zich echter van bewust dat er in de praktijk sterk uiteenlopende situaties en gegevensuitwisselingen denkbaar zijn waarbij een TTP een rol kan spelen. Vanuit die optiek behoudt zij zich steeds het recht voor om in concrete gevallen de modaliteiten voor de oprichting van een nieuwe TTP (of het gebruik van een bestaande TTP) te beoordelen op hun verenigbaarheid met de privacybeginselen.

Voor de Administrateur m.v., De Voorzitter,

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

[29] Tenzij desgevallend als verwerker, in opdracht van de instelling die de TTP-functie uitoefent.