Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid
Afdeling « Gezondheid »

SCSZ/11/072

BERAADSLAGING NR 11/047 VAN 21 JUNI 2011 MET BETREKKING TOT DE MEDEDELING VAN GECODEERDE PERSOONSGEGEVENS DOOR ZIEKENHUIZEN AAN DE FEDERALE OVERHEIDSDIENST VOLKSGEZONDHEID, VEILIGHEID VAN DE VOEDSELKETEN EN LEEFMILIEU IN HET KADER VAN EEN PROEFPROJECT INZAKE DE REGISTRATIE VAN PERSOONSGEGEVENS MET BETREKKING TOT DE SPOEDGEVALLENDIENSTEN

De afdeling gezondheid van het Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid (hierna "het Sectoraal Comité");

Gelet op de wet van 15 januari 1990 *houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid*, inzonderheid op artikel 37;

Gelet op de wet van 8 december 1992 *tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens;*

Gelet op de wet van 21 augustus 2008 *houdende oprichting en organisatie van het eHealth-platform*;

Gelet op de machtigingsaanvraag van de federale overheidsdienst Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu van 16 mei 2011;

Gelet op het auditoraatsrapport van 1 juni 2011;

Gelet op het verslag van de heer Yves Roger;

Beslist op 21 juni 2011, na beraadslaging, als volgt:

1. ONDERWERP VAN DE AANVRAAG

A. CONTEXT

1. In het kader van een proefproject inzake de registratie van gegevens met betrekking tot de spoedgevallendiensten, wenst de federale overheidsdienst Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu (hierna "FOD Volksgezondheid") vanwege de meewerkende ziekenhuizen de mededeling te bekomen van bepaalde gecodeerde persoonsgegevens. Die gegevens zullen de FOD in staat stellen om een beter zicht te krijgen op de werking van de spoedgevallendiensten en om, in geval van een crisis of een potentieel gevaarlijke situatie, de gepaste maatregelen te treffen.

2. Het Sectoraal Comité heeft reeds een machtiging verleend voor deze mededeling bij beraadslaging nr. 09/017 van 17 maart 2009, gewijzigd op 19 mei 2009, met betrekking tot de mededeling van gecodeerde persoonsgegevens door ziekenhuizen aan de federale overheidsdienst Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu in het kader van een pilootproject inzake de registratie van spoedgevallen[1].

   Deze machtiging werd echter slechts tot en met 1 maart 2010 verleend. Vandaar deze aanvraag.

B. DOELSTELLINGEN VAN DE REGISTRATIE

3. In geval van een crisis of van een potentieel gevaarlijke situatie dient de overheid immers snel over gegevens met betrekking tot de spoedgevallendiensten te kunnen beschikken, zodat ze snel de nodige (reactieve of preventieve) beslissingen kan nemen.

   Deze registratie zal dus nuttig zijn in geval van een nationale crisis (een vogelgrieppandemie, een nucleaire ramp, bioterrorisme, ...), een regionale crisis (een aardbeving, zware overstromingen, luchtvervuiling, ...) of een specifieke crisis (een voedselvergiftiging die haar oorsprong vindt in de voedingsindustrie, een luchtvaartramp, …) om de gevolgen van een dergelijke crisis zoveel mogelijk te beperken en in sommige gevallen zelfs om bepaalde van die gevolgen te voorkomen (bijvoorbeeld: tijdverlies bij de behandeling van de patiënten ingevolge een slechte doorsverwijzing naar de ziekenhuizen, alarmering van de gezondheidsnetwerken in verband met een potentiële dreiging, ...).

4. De registratie zal niet alleen in crisissituaties maar ook in de gewone praktijk toelaten om op basis van een permanente evaluatie van het gebruik van de beschikbare resources de nodige gepaste correctieve maatregelen te nemen, zowel op het niveau van het ziekenhuis als op regionaal en nationaal niveau en om snel de impact van deze maatregelen te kunnen evalueren.

[1] Beraadslaging nr. 09/017 van 17 maart 2009, gewijzigd op 19 mei 2009, met betrekking tot de mededeling van gecodeerde persoonsgegevens door ziekenhuizen aan de federale overheidsdienst Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu in het kader van een pilootproject inzake de registratie van spoedgevallen, beschikbaar op de website van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer, http://www.privacycommission.be/nl.

C. REGISTRATIE VAN DE PERSOONSGEGEVENS

1° De betreffende persoonsgegevens

5. De geregistreerde variabelen hebben zowel betrekking op de structuur van het ziekenhuis als op het medische, administratieve en sociale aspect van de patiënten. Naast de identificatie van het ziekenhuis (met behulp van het erkenningsnummer van het ziekenhuis, het vestigingsnummer en een beschrijving van de technische middelen) worden voor elke betrokken patiënt aldus de volgende gegevens gevraagd:

   - het identificatienummer dat door het ziekenhuis wordt gebruikt om de patiënt te identificeren (lokaal identificatienummer van de patiënt, hierna "LIP" genoemd). Dit nummer zal dubbel gecodeerd worden (zie *infra*);

   - het geboortejaar en de geboortemaand, het geslacht, de postcode van de verblijfplaats, de landcode van de verblijfplaats, de nationaliteitscode en de verzekerbaarheidscode;

   - persoonsgegevens met betrekking tot de opname op de spoedgevallendienst: de datum en het tijdstip van de opname, het type opname, de locatie vóór de opname, het kanaal waarlangs de betrokkene op de spoedgevallendienst is terechtgekomen, het type transportmiddel en de identificatie van het transportmiddel;

   - persoonsgegevens met betrekking tot het ontslag uit de spoedgevallendienst: de datum en het tijdstip van het ontslag, het type ontslag, de bestemming na het ontslag en het type opvolging;

   - persoonsgegevens met betrekking tot de problematiek: de reden van het contact met de spoedgevallendienst, de aard van het probleem (aanduiding van de dominante pathologiegroep) (een traumatologisch, medisch, chirurgisch, gynaecologisch, psychiatrisch dan wel sociaal probleem, een geval van intoxicatie, een contact met het oog op controle of een contact met het oog op het bekomen van een certificaat of van een voorschrift), de hoofddiagnose evenals de secundaire diagnose (globale groepen: cardiologie, dermatologie, neurologie, …), de verrichte diagnostische en therapeutische handelingen (bloedafname, radiografie, ECG, …), persoonsgegevens betreffende de gevallen van koolstofmonoxide-intoxicatie (type van intoxicatie, geschatte duur van blootstelling, eerste dosis koolstofmonoxide, zuurstofbehandeling, aanwezigheid van een koolstofmonoxidedetector, plaats van de intoxicatie en vermoedelijke oorzaak), het type ongeval en het type breuk.

6. In uitzonderlijke omstandigheden, meer bepaald indien de controle van de persoonsgegevens een abnormale statistische afwijking aan het licht brengt, zou de FOD Volksgezondheid wensen te beschikken over ad-hocpersoonsgegevens, om aldus de oorzaken van de vastgestelde afwijking te kunnen opsporen. Bij wintertoestand zou bijvoorbeeld kunnen worden gevraagd of er een toename is van het aantal opgenomen daklozen. De reden van een toename van de verblijfsduur op de spoedgevallendienst zou bijvoorbeeld ook kunnen worden gevraagd.

De lijst van deze bijkomende persoonsgegevens zou telkens op vraag van de Minister van Volksgezondheid of van de FOD Volksgezondheid worden opgesteld door twee geneesheren die gespecialiseerd zijn in de spoedgevallengeneeskunde en deel uitmaken van een ad-hoccommissie, samengesteld uit vertegenwoordigers van de FOD Volksgezondheid en vier geneesheren die gespecialiseerd zijn in de spoedgevallengeneeskunde.

2° Registratie van de betreffende persoonsgegevens

7. De betreffende persoonsgegevens worden door de deelnemende ziekenhuizen in hun informatiesysteem (*Hospital Information System* - HIS) ingevoerd. Vervolgens worden ze, na een dubbele codering van het LIP tot een gecodeerd identificatienummer van de patiënt (uniek betekenisloos volgnummer, hierna "GIP"), met behulp van een webservice (UREG) ter beschikking gesteld van de FOD Volksgezondheid. Vervolgens kunnen ze door de FOD in de daarvoor bestemde persoonsgegevensbank worden opgeslagen.

   De betreffende webservice is toegankelijk via de website van de FOD Volksgezondheid. Elk ziekenhuis zal enkel toegang hebben tot de eigen persoonsgegevens. De betrokkenen van de FOD Volksgezondheid zullen daarentegen toegang hebben tot alle geregistreerde gecodeerde persoonsgegevens.

8. Zoals hierboven aangegeven, zal het lokaal identificatienummer van de patiënt tweemaal gecodeerd worden. Het LIP wordt eerst door het ziekenhuis zelf gecodeerd tot een LCIP (Lokaal gecodeerd identificatienummer) Het LIP en het LCIP zijn dus enkel gekend door het ziekenhuis.

   Overeenkomstig de vereiste die het Sectoraal Comité in zijn beraadslaging nr. 09/017 van 17 maart 2009 stelt, wordt voortaan een beroep gedaan op de diensten van een intermediaire organisatie, met name het eHealth-platform, opgericht bij de wet van 21 augustus 2008 *houdende oprichting en organisatie van het eHealth-platform*[2], om het LCIP een tweede keer te coderen tot een GIP[3].

   De eindgebruikers bij de FOD Volksgezondheid beschikken dus enkel over het GIP.

9. De bij het proefproject betrokken ziekenhuizen worden via het gebruikers- en toegangsbeheer van het eHealth-platform geïdentificeerd en geauthentiseerd aan de hand van een eHealth-certificaat. Het Sectoraal comité heeft bij beraadslaging nr. 09/008 van 20 januari 2009 de machtiging verleend voor de toepassing van het geïntegreerd gebruikers- en toegangsbeheer door het eHealth-platform.

   De bij het proefproject betrokken ziekenhuizen zijn verantwoordelijk voor het verlenen van toegangsrechten aan en de identificatie en authenticatie van hun eigen medewerkers overeenkomstig de in de betrokken ziekenhuizen geldende methodes.

---

[2] Wet van 21 augustus 2008 *houdende oprichting en organisatie van het eHealth-platform*, B.S., 13 november 2008, p. 54454.

[3] Ter herinnering, in de oorspronkelijke beraadslaging was voorzien dat deze opdracht tijdelijk aan de FOD Volksgezondheid kon worden toevertrouwd.

De FOD Volksgezondheid staat in voor het toekennen van de toegang tot de gegevens aan zijn eigen gebruikers (een beperkt aantal medewerkers binnen de FOD Volksgezondheid die betrokken zijn bij dit proefproject).

2. BEVOEGDHEID

10. Ingevolge artikel 42, § 2, 3° van de wet van 13 december 2006 *houdende diverse bepalingen betreffende gezondheid*[4] is de afdeling gezondheid van het sectoraal comité van de sociale zekerheid en van de gezondheid in beginsel bevoegd voor het verlenen van een principiële machtiging met betrekking tot elke mededeling van persoonsgegevens die de gezondheid betreffen.

11. In artikel 11 van de wet van 21 augustus 2008 *houdende oprichting en organisatie van het eHealth-platform* wordt bepaald dat elke mededeling van persoonsgegevens door of aan het eHealth-platform, behoudens enkele uitzonderingsgevallen, een principiële machtiging van de afdeling gezondheid van het sectoraal comité van de sociale zekerheid en van de gezondheid vereist.

12. Overeenkomstig artikel 5, 8° van de wet van 21 augustus 2008 *houdende oprichting en organisatie van het eHealth-platform* vereist de tussenkomst van het eHealth-platform als intermediaire organisatie voor de koppeling en de codering van persoonsgegevens en de bewaring van het verband tussen het reële identificatienummer en het gecodeerd nummer de machtiging van het Sectoraal Comité.

13. Het Sectoraal Comité oordeelt bijgevolg dat het bevoegd is om zich uit te spreken over deze machtigingsaanvraag.

3. BEHANDELING VAN DE AANVRAAG

A. RECHTMATIGHEID

14. De verwerking van persoonsgegevens die de gezondheid betreffen is in beginsel verboden, overeenkomstig artikel 7, § 1 van de wet van 8 december 1992 *tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens* (hierna de "privacywet")[5].

15. Het verbod is echter niet van toepassing onder meer wanneer de verwerking noodzakelijk is voor de bevordering en de bescherming van de volksgezondheid[6]. In voorliggend geval lijkt de verwerking van de gecodeerde persoonsgegevens aldus gerechtvaardigd.

[4] Wet van 13 december 2006 *houdende diverse bepalingen betreffende gezondheid*, 22 december 2006, p. 73782.
[5] Wet van 8 december 1992 *tot bescherming van de persoonlijke levensfeer ten opzichte van de verwerking van persoonsgegevens, B.S.,* 18 maart 1993, p. 05801.
[6] Art. 7, § 2, d) van de privacywet.

B. FINALITEIT

16. Krachtens artikel 4, § 1, 2° van de privacywet is de verwerking van persoonsgegevens enkel toegelaten voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden.

17. De mededeling van gecodeerde persoonsgegevens door de deelnemende ziekenhuizen aan de FOD Volksgezondheid beantwoordt wel degelijk aan een gerechtvaardigd doeleinde. In geval van een crisis of een potentieel gevaarlijke situatie dient de FOD Volksgezondheid snel te kunnen beschikken over gegevens met betrekking tot de spoedgevallendiensten. Slechts dan is hij immers in staat om snel reactieve dan wel preventieve maatregelen te treffen.

C. PROPORTIONALITEIT

18. In artikel 4, § 1, 3° van de privacywet wordt bepaald dat de persoonsgegevens toereikend, terzake dienend en niet overmatig dienen te zijn, uitgaande van de doeleinden waarvoor zij worden verkregen of waarvoor zij verder worden verwerkt.

19. Om zijn opdracht te verwezenlijken, dient de FOD Volksgezondheid te kunnen beschikken over gecodeerde persoonsgegevens aangaande de patiënten van de spoedgevallendiensten van de deelnemende ziekenhuizen.

20. De mededeling van louter anonieme gegevens kan niet volstaan vermits analyses dienen te kunnen worden verricht aangaande de diverse spoedgevallen die zich in het ziekenhuis in kwestie hebben voorgedaan.

21. Zoals hierboven aangegeven, zal het LIP een eerste keer aan de bron worden gecodeerd, dat wil zeggen door het ziekenhuis, en het gecodeerde LIP, zijnde het LCIP, een tweede keer door het eHealth-platform.

22. Bovendien worden de eigenlijke persoonskenmerken, dat zijn de persoonsgegevens die het grootste risico op heridentificatie van de patiënt inhouden, in aantal beperkt (geboortejaar, geslacht, postcode, landcode, nationaliteitscode).

23. Zowel aangaande de opname op als het ontslag uit de spoedgevallendienst worden de exacte datum en het exacte tijdstip gevraagd. Hoewel het Sectoraal Comité doorgaans aandringt op de mededeling van data door een verwijzing naar de periode waarin ze vallen, erkent het in voorliggend geval het nut van een precieze mededeling. De FOD Volksgezondheid dient immers de exacte capaciteit en de werkelijke last van de onderscheiden spoedgevallendiensten te kennen.

24. Gelet op het voorgaande meent het Sectoraal Comité dat de voormelde gegevens als toereikend, ter zake dienend en niet-overmatig kunnen worden beschouwd uitgaande van de doeleinden waarvoor ze worden verkregen.

25. Het Sectoraal Comité is er zich van bewust dat de mededeling van de hogervermelde persoonsgegevens in sommige gevallen aanleiding zal geven tot een bijkomende mededeling van persoonsgegevens die niet vooraf kunnen worden gedefinieerd. Het

wenst hierbij te benadrukken dat bij een eventuele bijkomende mededeling van persoonsgegevens steeds rekening dient te worden gehouden met de beginselen vervat in de privacywet, in het bijzonder het proportionaliteitsbeginsel, ingevolge hetwelk persoonsgegevens, uitgaande van de doeleinden waarvoor ze worden meegedeeld, toereikend, ter zake dienend en niet-overmatig dienen te zijn.

26. Aldus dient de bijkomende mededeling te worden beperkt, enerzijds wat betreft het aantal personen op wie de persoonsgegevens betrekking hebben, anderzijds wat het aantal persoonsgegevens zelf betreft. Bij het opstellen van de lijst van bijkomend mee te delen persoonsgegevens dient er ook steeds rekening mee te worden gehouden dat ze niet tot gevolg mogen hebben dat het risico op heridentificatie van de betrokken personen zou vergroten.

27. Het sectoraal comité van de sociale zekerheid en van de gezondheid wenst in voorkomend geval op de hoogte te worden gehouden van dergelijke bijkomende mededeling.

D. TRANSPARANTIE

28. Overeenkomstig artikel 9, § 2 van de privacywet moet de verantwoordelijke voor de verwerking, indien de persoonsgegevens niet bij de betrokkene zijn verkregen, uiterlijk op het moment van de eerste mededeling van de gegevens bepaalde informatie verstrekken (de naam en het adres van de verantwoordelijke voor de verwerking, de doeleinden van de verwerking, …) aan de betrokkene.

29. De verantwoordelijke van de verwerking wordt echter vrijgesteld van deze informatieverstrekking indien « de kennisgeving aan de betrokkene onmogelijk blijkt of onevenredig veel moeite kost » [7]. In onderhavig geval is het Sectoraal Comité van oordeel dat de nodige inspanningen die door de FOD Volksgezondheid zullen moeten geleverd, als onevenredig kunnen worden beschouwd, rekening houdend met het aantal patiënten dat bij dit proefproject betrokken kan zijn (ongeveer 120.000 patiënten per jaar) en met de doelstelling van het project.

30. Rekening houdend met het voorgaande, oordeelt het Sectoraal Comité dat de uitzondering voorzien in artikel 9, § 2, tweede lid, van toepassing is.

E. VEILIGHEIDSMAATREGELEN

31. Overeenkomstig artikel 7, § 4 van de privacywet mogen persoonsgegevens betreffende de gezondheid enkel worden verwerkt onder de verantwoordelijkheid van een beroepsbeoefenaar in de gezondheidszorg.

32. Hoewel dit strikt genomen niet wordt vereist in de privacywet, verdient het volgens het Sectoraal Comité de voorkeur dat dergelijke gegevens worden verwerkt onder de verantwoordelijkheid van een geneesheer[8], wat in casu het geval is.

---

[7] Art. 9, § 2 van de privacywet.

[8] Het Sectoraal Comité heeft deze voorkeur opgesteld in zijn beraadslaging nr. 07/034 van 4 september 2007 met betrekking tot de mededeling van persoonsgegevens aan het Federaal Kenniscentrum voor de Gezondheidszorg

33. Het Comité herinnert eraan dat de beroepsbeoefenaar in de gezondheidszorg en zijn aangestelden of gemachtigden bij de verwerking van persoonsgegevens tot geheimhouding verplicht zijn[9].

34. Overeenkomstig artikel 16, § 4 van de privacywet moet de FOD Volksgezondheid alle gepaste technische en organisatorische maatregelen treffen die nodig zijn voor de bescherming van de persoonsgegevens. Deze maatregelen moeten een passend beveiligingsniveau verzekeren, rekening houdend, enerzijds, met de stand van de techniek ter zake en de kosten voor het toepassen van de maatregelen en, anderzijds, met de aard van de te beveiligen gegevens en de potentiële risico's.

35. Om de vertrouwelijkheid en de veiligheid van de gegevensverwerking te garanderen, dient elke instelling die persoonsgegevens bewaart, verwerkt of meedeelt maatregelen te treffen in de volgende tien actiedomeinen met betrekking tot de informatieveiligheid: veiligheidsbeleid; aanstelling van een informatieveiligheidsconsulent; organisatorische en menselijke aspecten van de veiligheid (vertrouwelijkheidsverbintenis van het personeel, regelmatige informatieverstrekking en opleidingen ten behoeve van het personeel inzake bescherming van de privacy en veiligheidsregels); fysieke veiligheid en veiligheid van de omgeving; netwerkbeveiliging; logische toegangs- en netwerkbeveiliging; loggings, opsporing en analyse van de toegangen; toezicht, nazicht en onderhoud; systeem van beheer van de veiligheidsincidenten en de continuïteit (*backup*-systemen, *fault tolerance*-systemen, …); documentatie[10].

36. Indien correct en volledig toegepast, acht het Sectoraal Comité de voormelde veiligheidsmaatregelen toereikend om de vertrouwelijkheid en de veiligheid van de gegevensverwerking te waarborgen in het licht van de bepalingen van de privacywet.

37. Het Sectoraal Comité herinnert eraan dat het overeenkomstig artikel 6 van 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*[11] verboden is om handelingen te stellen die ertoe strekken de meegedeelde gecodeerde persoonsgegevens om te zetten in niet-gecodeerde persoonsgegevens. Er wordt op gewezen dat het niet-naleven van dit verbod, krachtens artikel 39, 1° van de privacywet, een geldboete van honderd tot honderdduizend euro tot gevolg kan hebben. Het Sectoraal Comité herinnert er ook aan dat bij een veroordeling wegens een misdrijf omschreven in artikel 39 de rechter de verbeurdverklaring kan uitspreken van de dragers van persoonsgegevens waarop het misdrijf betrekking heeft (zoals manuele bestanden, magneetschijven of magneetbanden) of de uitwissing van die gegevens kan gelasten. De rechter kan ook het verbod opleggen om gedurende ten hoogste twee jaar rechtstreeks of door een tussenpersoon het beheer te hebben over enige verwerking van persoonsgegevens [12].

---

met het oog op het onderzoek 2007-16-HSR “Onderzoek naar mogelijke financieringsmechanismen voor het geriatrisch dagziekenhuis”.

[9] Art. 7, § 4 van de privacywet.

[10] “Referentiemaatregelen voor de beveiliging van elke verwerking van persoongegevens”, document opgesteld door de Commissie voor de Bescherming van de Persoonlijke Levenssfeer en beschikbaar op de volgende URL: http://www.privacycommission.be/nl/static/pdf/referenciemaatregelen-vs-01.pdf

[11] 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*, *B.S.*, 13 maart 2001, p. 07839.

[12] Artikel 41 van de privacywet.

F. TUSSENKOMST VAN HET eHEALTH-PLATFORM

38. Het eHealth-platform staat in voor de codering van het LCIP.

39. Krachtens artikel 5, 8° van de wet van 21 augustus 2008 *houdende oprichting en organisatie van het eHealth-platform* kan het eHealth-platform als intermediaire organisatie gegevens die nuttig zijn voor de kennis, de conceptie, het beheer en de verstrekking van gezondheidszorg inzamelen, samenvoegen, coderen of anonimiseren en ter beschikking stellen.

40. Het eHealth-platform kan deze opdracht enkel uitvoeren op vraag van bepaalde instanties, bijvoorbeeld op vraag van een federale overheidsdienst.

41. Bovendien mag het « de in het kader van deze opdracht verwerkte persoonsgegevens slechts bijhouden zolang dat noodzakelijk is om ze te coderen »[13]. Het eHealth-platform "mag evenwel het verband tussen het reële identificatienummer van een betrokkene en het aan hem toegekende gecodeerde identificatienummer bijhouden indien de bestemmeling van de gecodeerde persoonsgegevens daarom op een gemotiveerde wijze verzoekt, mits machtiging van het sectoraal comité van de sociale zekerheid en van de gezondheid"[14]. In dat opzicht stelt het Sectoraal Comité vast dat er in het kader van het proefproject geen nood is om het verband bij te houden.

Om deze redenen verleent

de afdeling gezondheid van het Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid

42. een machtiging aan de betrokken ziekenhuizen om gecodeerde persoonsgegevens op de hogervermelde wijze mee te delen aan de federale overheidsdienst Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu, met het oog het verwezenlijken van een proefproject inzake de registratie van persoonsgegevens betreffende de spoedgevallendiensten.

Yves ROGER
Voorzitter

[13] Art. 5, 8° van de wet van 21 augustus 2008 *houdende oprichting en organisatie van het eHealth-platform*, B.S., 13 oktober 2008, p. 54454.
[14] *Ibidem*.