

Informatieveiligheidscomité  
kamer federale overheid

**BERAADSLAGING NR. 20/043 VAN 6 OKTOBER 2020, GEWIJZIGD OP 7 DECEMBER 2021, MET BETREKKING TOT DE VERWERKING VAN GEPSEUDONIMISEERDE PERSOONSgegevens AFKOMSTIG VAN DE FOD FINANCIEN DOOR DE FOD SOCIALE ZEKERHEID VOOR DE ONTWIKKELING VAN HET MICROSIMULATIEMODEL BELMOD**

Gelet op de wet van 15 augustus 2012 *houdende oprichting en organisatie van een federale dienstenintegrator*, in het bijzonder artikel 35/1;

Gelet op de wet van 3 december 2017 *tot oprichting van de Gegevensbeschermingsautoriteit*, in het bijzonder artikel 114;

Gelet op de wet van 5 september 2018 *tot oprichting van het informatieveiligheidscomité en tot wijziging van diverse wetten betreffende de uitvoering van verordening (EU) 2016/679 van 27 april 2016 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van richtlijn 95/46/EG*, in het bijzonder artikel 98;

Gelet op de aanvraag de Federale Overheidsdienst Sociale Zekerheid;

Gelet op het rapport van de federale overheidsdienst Beleid en Ondersteuning;

Gelet op het verslag van de voorzitter.

**A. ONDERWERP VAN DE AANVRAAG**

1. De Federale Overheidsdienst Sociale Zekerheid heeft in het verleden de toelating verkregen van het voormalig Sectoraal comité van de sociale zekerheid en van de gezondheid en van het Informatieveiligheidscomité om gepseudonimiseerde persoonsgegevens te ontvangen uit het Datawarehouse Arbeidsmarkt en Sociale Bescherming van de Kruispuntbank van de Sociale Zekerheid (beraadslaging nr. 17/020 van 7 maart 2017, gewijzigd op 6 juni 2017 en op 14 januari 2020) en uit de IPCAL-databank (belastinggegevens) en STIPAD/CADNET-databank (kadastraal inkomen) van de FOD Financiën (beraadslaging nr. 19/037 van 5 november 2019) teneinde het microsimulatiemodel MIMOSIS te ontwikkelen.
2. MIMOSIS (*MI*cro*simulation MO*del for Belgian Social Security Systems) is een microsimulatiemodel voor sociaal beleid in België en maakt het mogelijk om hervormingen in een aantal beleidsdomeinen van de sociale zekerheid te simuleren op basis van

geanonimiseerde maar individuele administratieve gegevens uit voormelde databanken. MIMOSIS richt zich op 6 beleidsdomeinen: sociale zekerheidsbijdragen, pensioenen, werkloosheidsuitkeringen, bijstandsuitkeringen, ziekte- en invaliditeitsuitkeringen en gezinsbijslagen. Voor elke hervorming wordt via een geïntegreerde belastingmodule tevens het effect berekend op de verschuldigde personenbelasting. Door het gebruik van microgegevens laat het model een zeer gedetailleerde impactanalyse toe van de budgettaire en verdelingseffecten van wijzigingen in een aantal domeinen van de sociale zekerheid.

3. De federale overheidsdienst Sociale Zekerheid streeft thans naar een modernisering van het huidig microsimulatiemodel voor de sociale zekerheid. Hiervoor heeft hij in het kader van het BELMOD-project een samenwerking opgezet met de Universiteit Antwerpen, de Katholieke Universiteit Leuven en het Federaal Planbureau. Het nieuwe microsimulatiemodel BELMOD zou de gebruiksvriendelijkheid van EUROMOD (het microsimulatiemodel van de Europese Unie) en de accuraatheid van MIMOSIS (het Belgisch microsimulatiemodel) combineren en de mogelijkheid bieden om meer beleidsdomeinen op een nauwkeurigere wijze te simuleren. BELMOD moet een state-of-the-art microsimulatiemodel worden waarmee de impact van nieuwe beleidsmaatregelen vooraf kan worden geëvalueerd.
4. Voor de ontwikkeling van BELMOD willen de federale overheidsdienst Sociale Zekerheid (als verwerkingsverantwoordelijke) en de Universiteit Antwerpen, de Katholieke Universiteit Leuven en het Federaal Planbureau (als verwerkers) elk afzonderlijk – in hun eigen lokalen – gebruik kunnen maken van de persoonsgegevens die eerder, met toepassing van de hogervermelde beraadslagingen, aan de federale overheidsdienst Sociale Zekerheid werden overgemaakt voor de ontwikkeling van het microsimulatiemodel MIMOSIS. Het gaat om de persoonsgegevens van een door de federale overheidsdienst Sociale Zekerheid zelf te trekken steekproef van 30% van de oorspronkelijke populatie. Die persoonsgegevens zouden worden gepseudonimiseerd (dat wil zeggen ontdaan van elk element dat zonder afzonderlijk bewaarde informatie tot een koppeling met een specifieke betrokkene zou kunnen leiden) maar ten aanzien van de verwerkers ook door de federale overheidsdienst Sociale Zekerheid worden gescrambled (dat wil zeggen door elkaar gehaald, vaag gemaakt of ontdaan van gevoelige informatie, op een dergelijke wijze dat de originele gegevens niet meer kunnen bepaald worden op basis van de gescramblede gegevens).
5. Mits toestemming van het informatieveiligheidscomité zouden de onderzoekers van de federale overheidsdienst Sociale Zekerheid en diens verwerkers aldus gebruik kunnen maken van de gepseudonimiseerde en (wat de verwerkers betreft) gescramblede persoonsgegevens van ongeveer één derde van de originele populatie. Elke partner/verwerker van het project (de Universiteit Antwerpen, de Katholieke Universiteit Leuven en het Federaal Planbureau) zou – zij het enkel tijdens de fase van de ontwikkeling van BELMOD – in de eigen omgeving kunnen beschikken over die persoonsgegevens.
6. De federale overheidsdienst Sociale Zekerheid zou instaan voor het trekken van de steekproef van 30% van de oorspronkelijke populatie en het scramblen van de persoonsgegevens van de steekproefpersonen. Hij zou die bewerkte persoonsgegevens vervolgens overmaken aan de Kruispuntbank van de Sociale Zekerheid, die ze op haar beurt aan de drie partners/verwerkers zou bezorgen (de Kruispuntbank van de Sociale Zekerheid bezit immers de geschikte servers en tools om de persoonsgegevens op een veilige wijze ter beschikking te stellen).

7. In de aanvraag wordt opgemerkt dat elke BELMOD-partner verantwoordelijk is voor het ontwikkelen van bepaalde beleidsmodules. De ontwikkeling van het model blijkt een langdurig en intensief proces dat een constante (dagelijkse) validatie van de resultaten vereist. Het uitwerken van de verschillende modules en het ontwikkelen van de inputdataset vormen een iteratief proces waarbij het voor elke onderzoeker/ontwikkelaar noodzakelijk is om een zeer gedetailleerd inzicht in de onderliggende data te verwerven. Bovendien overlappen de inputgegevens voor de verschillende modules elkaar, waardoor nauwe samenwerking tussen de partners vereist is.
8. De ontwikkelingsfase van het BELMOD-project loopt tot 2022. De onderzoekers moeten de ontvangen gepseudonimiseerde en gescramblede persoonsgegevens uiterlijk op 30 juni 2022 vernietigen. In de loop van 2022 zou bij het informatieveiligheidscomité een nieuwe beraadslaging aangevraagd worden voor de verwerking van persoonsgegevens tijdens de exploitatiefase van het model. Er zou daarbij worden onderzocht of het mogelijk is om zowel het BELMOD-model als de BELMOD-dataset te plaatsen op een platform waarbij gebruikers vanop afstand met het model kunnen werken. Daarom moet in de ontwikkelingsfase het model door alle onderzoekers ontwikkeld worden binnen een gemeenschappelijk platform bepaald door de FOD SZ, zodat er later geen nood is om de gegevens meervoudig te blijven opslaan. Bij ieder van de 3 onderzoeksteams wordt er op 1 server gewerkt, zonder mogelijkheid tot downloaden van gegevens op aparte PC's.
9. Elke onderzoeker zou vooraf worden ingelicht over de relevante regelgeving en over de sanctionering bij de niet-naleving ervan. De gegevens mogen door de onderzoekers enkel worden gebruikt voor de modelbouw, niet voor andere doeleinden. Er zal een verwerkersovereenkomst worden opgesteld tussen de verwerkingsverantwoordelijke en elke verwerker overeenkomstig de GDPR. Enkel zij die een vertrouwelijkheidscontract hebben ondertekend en er zich aldus toe hebben verbonden om de veiligheid en de vertrouwelijkheid van de ontvangen persoonsgegevens te bewaren, zouden toegang tot de persoonsgegevens krijgen voor het ontwikkelen van het nieuwe microsimulatiemodel. Tijdens het project zou steeds een actuele lijst worden bijgehouden van de personen die toegang hebben. Daarenboven voorzien de verwerkers (de Universiteit Antwerpen, de Katholieke Universiteit Leuven en het Federaal Planbureau) elk specifieke veiligheidsmaatregelen.
10. De verwerking van de persoonsgegevens afkomstig van het Datawarehouse Arbeidsmarkt en Sociale Bescherming van de KSZ door de FOD Sociale Zekerheid en haar verwerkers in het licht van de ontwikkeling van het microsimulatiemodel BELMOD werd door de kamer sociale zekerheid en gezondheid van het Informatieveiligheidscomité goedgekeurd bij beraadslaging nr. 20/116 van 31 juli 2020.

## **II. ONDERZOEK VAN DE AANVRAAG**

### **A. ONTVANKELIJKHEID EN BEVOEGDHEID VAN HET COMITE**

11. Krachtens artikel 35/1, §1, eerste lid, van de wet van 15 augustus 2012 *houdende oprichting en organisatie van een federale dienstenintegrator* vergt de mededeling van persoonsgegevens door overheidsdiensten en openbare instellingen van de federale overheid aan andere derden dan de instellingen van sociale zekerheid bedoeld in artikel 2, eerste lid, 2°, van de wet van 15 januari 1990 *houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid*, een voorafgaande beraadslaging van de kamer

federale overheid van het informatieveiligheidscomité, voor zover de verwerkingsverantwoordelijken van de meedelende instantie en de ontvangende instanties, in uitvoering van artikel 20 van de wet van 30 juli 2018 *betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens*, niet tot een akkoord komen over de mededeling of minstens één van die verwerkingsverantwoordelijken om een beraadslaging verzoekt.

12. Het Informatieveiligheidscomité stelt vast dat de FOD Sociale Zekerheid reeds beschikt over de betreffende persoonsgegevens, initieel afkomstig van de FOD Financiën<sup>1</sup>, doch dat de FOD Sociale Zekerheid de gegevens thans voor een ander doeleinde wil aanwenden en ze wil meedelen aan instanties die zullen optreden als verwerker van de FOD Sociale Zekerheid dewelke op haar beurt optreedt als verwerkingsverantwoordelijke.
13. Gelet op het voorgaande acht de kamer Federale Overheid zich dan ook bevoegd om zich over de aanvraag uit te spreken.

## **B. TEN GRONDE**

### **B.1. VERANTWOORDINGSPLICHT**

14. Overeenkomstig artikel 5.2 van de Algemene Verordening Gegevensbescherming<sup>2</sup> (hierna ‘AVG’ genoemd) is de FOD Financiën (de initieel meedelende instantie) en de FOD Sociale Zekerheid (initieel ontvangende instantie) als verwerkingsverantwoordelijken verantwoordelijk voor het naleven van de beginselen van de AVG en moeten ze in staat zijn dit aan te tonen.
15. Het Informatieveiligheidscomité wijst erop dat iedere verantwoordelijke voor de verwerking een register van de verwerkingsactiviteiten die onder zijn verantwoordelijkheid plaatsvinden, moet bijhouden overeenkomstig de voorwaarden opgenomen in artikel 30 AVG. De verschillende modaliteiten van het hergebruik van de reeds ontvangen persoonsgegevens dienen bijgevolg bijkomend in het register van verwerkingsactiviteiten
16. De FOD Sociale Zekerheid dient als verwerkingsverantwoordelijke bovendien een overeenkomst in de zin van artikel 28 van de Algemene Verordening Gegevensbescherming af te sluiten met zijn verwerkers.

### **B.2. RECHTMATIGHEID**

17. Overeenkomstig art. 5.1 a) AVG moeten persoonsgegevens worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig is. Dit houdt in dat de beoogde verwerking een basis moet vinden in één van de rechtmatigheidsgronden vermeld in artikel 6 AVG.
18. Het Comité stelt vast dat de verwerking overeenkomstig art. 6, §1, e), AVG noodzakelijk is voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen. Overeenkomstig het koninklijk besluit van 23 mei 2001 *houdende oprichting van de Federale Overheidsdienst Sociale Zekerheid*, heeft de FOD Sociale Zekerheid heeft volgende

---

<sup>1</sup> De mededeling van de persoonsgegevens werd toegelaten bij beraadslaging nr. 19/037 van 5 november 2019 van de kamer Federale Overheid van het Informatieveiligheidscomité.

<sup>2</sup> Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG.

strategische opdrachten: coördinatie en ondersteuning van het sociaal beleid, aanbod van sociale dienstverlening aan de gebruikers en bestrijding van sociale fraude. Het Directoraat-Generaal Beleidsondersteuning- en coördinatie van de FOD Sociale Zekerheid biedt de sleutelactoren van de politieke besluitvorming inzake sociale bescherming in België (ministers en staatssecretarissen, sociale partners, OISZ) de nodige ondersteuning (coördinatie, regelgeving, studies, analyses, budgettering, valorisatie, indicatoren, internationale vertegenwoordiging) bij de besluitvorming. De ontwikkeling en het gebruik van een microsimulatiemodel maakt hier een essentieel onderdeel van uit.

15. Gelet op het voorgaande, acht het Informatieveiligheidscomité de beoogde verwerking van persoonsgegevens rechtmatig.

### **B.3. DOELBINDING**

16. Artikel 5.1 b) AVG laat de verwerking van persoonsgegevens slechts toe voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden (principe van doelbinding). De gegevens mogen bovendien niet verder worden verwerkt op een wijze die onverenigbaar is met die doeleinden.
17. De verwerking van de persoonsgegevens in kwestie heeft tot doel om de FOD Sociale Zekerheid (als verwerkingsverantwoordelijke) samen met de Universiteit Antwerpen, de Katholieke Universiteit Leuven en het Federaal Planbureau (als verwerkers) toe te laten een nieuw microsimulatiemodel voor de sociale zekerheid te ontwikkelen en om de impact van nieuwe beleidsmaatregelen vooraf te evalueren. In de ontwikkelingsfase van het nieuw microsimulatiemodel BELMOD bezorgt de federale overheidsdienst Sociale Zekerheid daartoe met de tussenkomst van de Kruispuntbank van de Sociale Zekerheid aan de hogervermelde organisaties enige gepseudonimiseerde en gescramblede persoonsgegevens op basis van de gepseudonimiseerde persoonsgegevens die de federale overheidsdienst Sociale Zekerheid eerder ontving voor het microsimulatiemodel voor de sociale zekerheid MIMOSIS.
18. Gelet op het voorgaande acht het Informatieveiligheidscomité de doeleinden van de beoogde mededeling van persoonsgegevens als welbepaald, uitdrukkelijk omschreven en gerechtvaardigd. Ze zijn niet onverenigbaar met de doeleinden waarvoor de FOD Sociale Zekerheid de persoonsgegevens initieel had ontvangen. De gegevens mogen door de onderzoekers enkel worden gebruikt voor de modelbouw van het nieuwe microsimulatiemodel, niet voor andere doeleinden.

### **B.4. PROPORTIONALITEIT**

#### **B.4.1. Minimale gegevensverwerking**

19. Artikel 5.1 b) AVG stelt dat persoonsgegevens ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt, moeten zijn (“minimale gegevensverwerking”).
20. De gepseudonimiseerde en gescramblede persoonsgegevens hebben betrekking op een steekproef van 30% van de gezinnen waarover de federale overheidsdienst Sociale Zekerheid reeds persoonsgegevens verwerkt in het kader van het microsimulatiemodel voor de sociale zekerheid MIMOSIS (aangaande een oorspronkelijke populatie van ongeveer vierhonderdduizend steekproefpersonen en hun respectieve gezinsleden). De Universiteit Antwerpen, de Katholieke Universiteit Leuven en het Federaal Planbureau kunnen per aldus geselecteerde betrokken referentiepersoon (en zijn gezinsleden) beschikken over dezelfde

(weliswaar door scrambling bewerkte) persoonsgegevens, in hun eigen lokalen, zij het steeds overeenkomstig de bepalingen van artikel 28 van de Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG over de relatie tussen de verwerkingsverantwoordelijken en de verwerkers.

21. Het Informatieveiligheidscomité stelde in zijn beraadslaging nr. 17/020 van 7 maart 2017, gewijzigd op 6 juni 2017 en op 14 januari 2020 (wat de gegevens afkomstig van het Datawarehouse Arbeidsmarkt en Sociale Bescherming van de KSZ betreft), en zijn beraadslaging nr. 19/037 van 5 november 2019 (wat de gegevens afkomstig van de FOD Financiën) vast dat de initiële mededeling aan de federale overheidsdienst Sociale Zekerheid betrekking had op een groot aantal persoonsgegevens maar dat die niettegenstaande hun omvangrijk aantal op zich niet van die aard waren om te leiden tot een heridentificatie van de betrokkenen, behalve in het nooit volledig uit te sluiten geval van voorkennis in hoofde van de onderzoekers (indirecte contextuele heridentificatie). Dat oordeel geldt tevens voor de mededeling van dezelfde gepseudonimiseerde persoonsgegevens van een steekproef van 30% van de gezinnen uit de initiële populatie aan de diverse partners van het BELMOD-project, temeer omdat de persoonsgegevens gescrambled worden.
26. Gelet op het voorgaande, acht het Informatieveiligheidscomité de persoonsgegevens ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt, rekening houdend met de doeleinden waarvoor de persoonsgegevens zullen worden verwerkt.

#### **B.4.2. Opslagbeperking**

27. Aangaande de bewaringstermijn herinnert het Comité er aan dat persoonsgegevens niet langer mogen worden bewaard in een vorm die het mogelijk maakt de betrokkenen te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is.
28. De verwerkingsverantwoordelijke en zijn drie verwerkers (de Universiteit Antwerpen, de Katholieke Universiteit Leuven en het Federaal Planbureau) mogen de meegedeelde gepseudonimiseerde persoonsgegevens bewaren zolang hun verwerking noodzakelijk is in het kader van de ontwikkeling van het BELMOD-project en uiterlijk tot 30 juni 2022. Daarna dienen zij te worden vernietigd.

#### **B.5. BEVEILIGING**

29. Persoonsgegevens moeten door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging („integriteit en vertrouwelijkheid”).
30. Het microsimulatiemodel MIMOSIS en de persoonsgegevens die ervoor aangewend worden, zijn door de federale overheidsdienst Sociale Zekerheid op beveiligde *stand alone personal computers* geïnstalleerd met het oog op de exploitatie ervan. Derden kunnen deze persoonsgegevens als verwerker van de federale overheidsdienst Sociale Zekerheid

gebruiken voor exploitatiedoeleinden, maar enkel op dezelfde binnen de federale overheidsdienst Sociale Zekerheid geïnstalleerde beveiligde personal computers.

- 31.** Voor de ontwikkeling van het nieuwe microsimulatiemodel BELMOD wordt een andere werkwijze gevolgd. Tijdelijk – tot uiterlijk 30 juni 2022 – beschikken de partners (de Universiteit Antwerpen, de Katholieke Universiteit Leuven en het Federaal Planbureau) in hun eigen vertrekken over een deel van de gepseudonimiseerde persoonsgegevens waarover de federale overheidsdienst Sociale Zekerheid reeds beschikt. De federale overheidsdienst Sociale Zekerheid scramblert deze persoonsgegevens vooraleer ze via de Kruispuntbank van de Sociale Zekerheid over te maken aan de partners. De federale overheidsdienst Sociale Zekerheid dient te worden beschouwd als verwerkingsverantwoordelijke. In de ontwikkelingsfase moet het model door alle onderzoekers ontwikkeld worden binnen een gemeenschappelijk platform bepaald door de federale overheidsdienst Sociale Zekerheid, zodat er later geen nood is om de gegevens meervoudig te blijven opslaan.
- 32.** De resultaten van de verwerking mogen niet worden bekendgemaakt in een vorm die de identificatie van de betrokken persoon mogelijk maakt. De persoonsgegevens mogen voorts niet verder worden meegedeeld aan derden behalve indien het informatieveiligheidscomité daartoe uitdrukkelijk zijn goedkeuring verleent. Bij ieder van de 3 onderzoeksteams wordt er op 1 server gewerkt, zonder mogelijkheid tot downloaden van gegevens op aparte PC's.
- 33.** Het Comité wijst erop dat artikel 35 AVG in bepaalde gevallen vereist dat de verwerkingsverantwoordelijke vóór de verwerking een beoordeling uitvoert van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens. Het Comité verwijst hieromtrent naar de 'Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking "waarschijnlijk een hoog risico inhoudt" in de zin van Verordening 2016/679' van de Groep Gegevensbescherming Artikel 29 en de aanbeveling uit eigen beweging nr. 01/2018 van 28 februari 2018 van de Commissie voor de bescherming van de persoonlijke levenssfeer met betrekking tot de gegevensbeschermingseffectbeoordeling en voorafgaande raadpleging .
- 34.** Indien uit deze beoordeling zou blijken dat bijkomende maatregelen moeten worden getroffen, dienen de betrokken partijen op eigen initiatief een aanvraag tot wijziging van onderhavige beraadslaging in. De mededeling van persoonsgegevens mag in voorkomend geval niet plaatsvinden totdat de vereiste toelating van het Comité is bekomen. Indien uit de gegevensbeschermingseffectbeoordeling zou blijken dat er een hoog residuair risico is, dient de aanvrager de beoogde gegevensverwerking voor te leggen aan de Gegevensbeschermingsautoriteit, overeenkomst art. 36.1 AVG.

Om deze redenen besluit

**de kamer federale overheid van het Informatieveiligheidscomité**

dat de verwerking van gepseudonimiseerde persoonsgegevens afkomstig van de FOD Financiën door de FOD Sociale Zekerheid voor de ontwikkeling van het microsimulatiemodel BELMOD toegestaan is, mits wordt voldaan aan de vastgestelde maatregelen ter waarborging van de gegevensbescherming, in het bijzonder de maatregelen op het vlak van doelbinding, minimale gegevensverwerking, opslagbeperking en informatieveiligheid.

Het Informatieveiligheidscomité wijst erop dat de verwerkingsverantwoordelijke gehouden is om in voorkomend geval een gegevensbeschermingseffectbeoordeling uit te voeren. Als uit die beoordeling zou blijken dat bijkomende maatregelen moeten worden getroffen om de rechten en vrijheden van de betrokkenen te vrijwaren, dan zijn de partijen ertoe gehouden om de gewijzigde modaliteiten van de gegevensverwerking ter beraadslaging aan het Informatieveiligheidscomité voor te leggen.

B. PRENEEL  
kamer federale overheid

De zetel van de kamer federale overheid van het Informatieveiligheidscomité is gevestigd in de kantoren van de FOD Beleid en Ondersteuning, op volgend adres: Simon Bolivarlaan 30, 1000 Brussel.
---