

**Art. 8.** Sans préjudice des compétences des officiers de la police judiciaire, les fonctionnaires désignés par le Gouvernement flamand surveillent le respect du présent décret et des arrêtés d'exécution.

Ils sont habilités à constater les infractions commises à l'égard du présent décret et de ses arrêtés d'exécution au moyen d'un procès-verbal faisant foi jusqu'à la preuve du contraire. Une copie du procès-verbal est envoyée aux contrevenants dans le mois suivant la constatation de l'infraction.

Dans le cadre de l'exercice de leur mission, ils peuvent :

- 1° accéder à des locaux, des terrains et des moyens de transport;
- 2° réquisitionner des renseignements et des copies à fournir par les personnes interrogées et consulter les informations contenues dans des documents et sur d'autres supports;
- 3° se faire accompagner de personnes désignées par eux à cet effet en raison de leur expertise;
- 4° demander l'assistance de la police.

Il est obligatoire de fournir aux personnes en charge de la surveillance, dans un délai raisonnable fixé par eux, toute la collaboration qu'ils peuvent demander raisonnablement dans l'exercice de leurs compétences.

**Art. 9.** A la suite du constat d'une infraction au présent décret ou à ses arrêtés d'exécution, les personnes chargées de la surveillance, visées à l'article 8, peuvent :

- 1° interdire à un bateau ou à un autre véhicule l'accès à ou le séjour dans le port;
- 2° arrêter un bateau ou un autre véhicule et l'emmener ou le faire emmener vers un lieu à proximité;
- 3° interdire à un bateau ou à un autre véhicule de prendre la mer;
- 4° écarter d'office un bateau, un autre véhicule ou des marchandises dangereuses;
- 5° faire interrompre les opérations de chargement et de déchargement.

Promulguons le présent décret, ordonnons qu'il soit publié au *Moniteur belge*  
Bruxelles, le 6 juillet 2012.

Le ministre-président du Gouvernement flamand,  
K. PEETERS

La ministre flamande de la Mobilité et des Travaux publics,  
H. CREVITS

—  
Note

(1) *Session 2011-2012.*

*Documents* : - Projet de décret : 1600 — N° 1  
- Rapport : 1600 — N° 2  
- Texte adopté en séance plénière : 1600 — N° 3

*Annales* - Discussion et adoption : séance du 27 juin 2012.

---

## VLAAMSE OVERHEID

N. 2012 — 2234

[C — 2012/35894]

### 13 JULI 2012. — Decreet houdende de oprichting en organisatie van een Vlaamse dienstenintegrator (1)

Het VLAAMS PARLEMENT heeft aangenomen en Wij, REGERING, bekrachtigen hetgeen volgt :

Decreet houdende de oprichting en organisatie van een Vlaamse dienstenintegrator

#### HOOFDSTUK 1. — Algemene bepalingen

**Artikel 1.** Dit decreet regelt een gemeenschaps- en gewestaangelegenheid.

**Art. 2.** In dit decreet wordt verstaan onder :

1° authentieke gegevensbron : een authentieke gegevensbron als vermeld in artikel 4, § 1 en § 2, van het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer;

2° de Vlaamse toezichtcommissie : de Vlaamse toezichtcommissie, opgericht bij artikel 10 van het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer;

3° dienstenintegrator : een instantie die bij of krachtens een wet, een decreet of een ordonnantie belast is, binnen een bepaald overheidsniveau of in een bepaalde sector, met een taak van algemeen belang, en meer bepaald met de organisatie van elektronische gegevensuitwisseling over instanties heen en met de geïntegreerde ontsluiting van gegevens;

4° externe overheid : een overheid die tot het internationale of federale niveau behoort, een andere gemeenschap of een ander gewest, en de daarvan afhangende instellingen of rechtspersonen, alsook de privaatrechtelijke rechtspersonen die belast zijn met taken of opdrachten van algemeen belang;

5° het besluit van de Vlaamse Regering van 15 mei 2009 betreffende de veiligheidsconsulenten : het besluit van de Vlaamse Regering van 15 mei 2009 betreffende de veiligheidsconsulenten, vermeld in artikel 9 van het decreet van 18 juli 2008;

6° instanties : de instanties, vermeld in artikel 4, § 1, van het decreet van 26 maart 2004 betreffende de openbaarheid van bestuur;

7° machtiging : de machtiging, vermeld in artikel 8 van het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer, verleend door de Vlaamse toezichtcommissie of het bevoegde sectoraal comité naar gelang de elektronische mededeling van persoonsgegevens onderworpen is aan een machtiging van de Vlaamse toezichtcommissie of een sectoraal comité;

8° sectoraal comité : een sectoraal comité, opgericht binnen de Commissie voor de bescherming van de persoonlijke levenssfeer overeenkomstig artikel 31 bis van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens;

9° VDI : de Vlaamse dienstenintegrator.

#### HOOFDSTUK 2. — Oprichting van de VDI

**Art. 3.** § 1. De DAB Informatie Vlaanderen, vermeld in artikel 79 van het decreet van 22 december 2006 houdende bepalingen tot begeleiding van de begroting 2007, vervult de functie van dienstenintegrator met als doel de gegevensuitwisseling te vereenvoudigen en te optimaliseren tussen de instanties onderling enerzijds en tussen de instanties en de andere dienstenintegratoren en externe overheden anderzijds.

De VDI ondersteunt de instanties door een onderlinge elektronische dienstverlening en gegevensuitwisseling te organiseren tussen de instanties onderling, tussen de instanties en de externe overheden, en tussen de instanties en de andere dienstenintegratoren, om de instanties in staat te stellen de opdrachten voor de gebruikers van de door hen aangeboden diensten uit te voeren op een effectieve en efficiënte wijze, met een minimum aan administratieve lasten en kosten. De eenmalige inzameling en een gecoördineerde ontsluiting van de gegevens staan centraal bij de werking van de VDI.

De VDI organiseert de elektronische dienstverlening en gegevensuitwisseling met waarborgen op het vlak van de informatieveiligheid en de bescherming van de persoonlijke levenssfeer en in nauw overleg met de instanties, externe overheden en de andere dienstenintegratoren.

§ 2. In afwijking van paragraaf 1, ondersteunt de VDI niet de elektronische dienstverlening en de gegevensuitwisselingen die bij of krachtens een wet, een decreet of een ordonnantie door een andere dienstenintegrator gebeuren.

De VDI stroomlijnt in overleg met andere dienstenintegratoren de gegevensuitwisseling, vermeld in paragraaf 1.

§ 3. Behoudens andersluidende decretale of reglementaire bepalingen verleent de VDI geen aanvullende rechten aan personen of instanties tot raadpleging, mededeling of enige andere verwerking van gegevens bovenop de toepasselijke decretale en reglementaire bepalingen.

#### HOOFDSTUK 3. — Opdrachten en werking van de VDI

**Art. 4.** De VDI is voor de uitvoering van zijn doel belast met de volgende opdrachten :

1° een visie en een strategie ontwikkelen voor een effectieve, efficiënte en goed beveiligde elektronische dienstverlening en gegevensuitwisseling, vermeld in artikel 3, en het opvolgen van de naleving ervan;

2° de homogeniteit en consistentie van het beleid met de strategie, vermeld in punt 1°, bevorderen en bewaken;

3° een centraal gegevensuitwisselingsplatform concipiëren, ontwikkelen en beheren, dat bestaat uit generieke ICT-diensten en -infrastructuur, en dat de gegevensuitwisseling tussen de verschillende gegevensbronnen, beheerd door instanties of externe overheden, op een generieke manier mogelijk maakt;

4° nuttige basisdiensten concipiëren, ontwikkelen en ter beschikking stellen om de elektronische gegevensuitwisseling te ondersteunen, zoals een systeem voor de organisatie en logging van elektronische gegevensuitwisseling, een systeem voor elektronische toegang tot gegevens, een systeem voor gebruikers- en toegangsbeheer, een systeem voor elektronische datering en een systeem voor codering en anonimisering van gegevens;

5° aan de hand van een taakverdeling tussen alle betrokken partijen duidelijke afspraken maken over :

a) wie welke authenticaties, verificaties en controles verricht aan de hand van welke middelen en wie daarvoor de verantwoordelijkheid draagt;

b) hoe tussen de betrokken partijen de resultaten van de verrichte authenticaties, verificaties en controles op een veilige wijze elektronisch worden bewaard en uitgewisseld;

c) wie welke loggings bijhoudt;

d) hoe ervoor wordt gezorgd dat bij onderzoek, op initiatief van een betrokken partij of van een controleorgaan of naar aanleiding van een klacht, volledig kan gereconstrueerd worden welke natuurlijke persoon welke dienst of transactie omtrent welke burger of onderneming wanneer heeft gebruikt, via welk kanaal en voor welke doeleinden;

6° overeenkomstig de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, een verwijzingsrepertorium beheren, waarin aangegeven wordt bij welke instanties welke types van gegevens worden bewaard over welke personen, ondernemingen of instellingen, of dat verwijst naar de gegevensbron waar die gegevens kunnen worden geraadpleegd, of dat per natuurlijke persoon of onderneming aangeeft welke soorten gegevens ter beschikking worden gesteld aan welke instanties of externe overheden voor welke periode, met vermelding van het doel waarvoor de instantie of externe overheid die gegevens nodig heeft, en een autorisatierepertorium beheren dat bepaalt wie onder welke voorwaarden toegang krijgt tot welke gegevens. Het verwijzings- en autorisatierepertorium kan pas geïmplementeerd worden na advies van de Vlaamse toezichtcommissie;

7° instanties begeleiden bij de implementatie van de strategie, vermeld in punt 1°;

8° nuttige ICT-gerelateerde functionele en technische normen, standaarden, specificaties en basisarchitectuur die goedgekeurd zijn door het coördinatiecomité, vermeld in artikel 20, uitwerken en invoeren om ICT efficiënt in te zetten ter ondersteuning van de visie en strategie, vermeld in punt 1°, en het opvolgen van de naleving ervan;

9° ICT-gerelateerde, organisatorische, functionele en technische aspecten van gegevensuitwisseling beheren en coördineren;

10° programma's, projecten en diensten uitwerken die potentieel de instanties overkoepelen en die de gemeenschappelijke strategie, vermeld in punt 1°, ondersteunen;

11° de Verrijkte Kruispuntbank van Ondernemingen, afgekort VKBO, beheren. De VKBO is een gegevensbron waarin identificatiegegevens van ondernemingen uit de Kruispuntbank van Ondernemingen worden opgeslagen en verrijkt met ondernemingsgegevens uit verschillende gegevensbronnen, beheerd door andere instanties en externe overheden. De gegevens, opgeslagen in de VKBO, worden ter beschikking gesteld aan instanties en externe overheden om de opdrachten uit te voeren die hun door of krachtens een wet, een decreet of een ordonnantie zijn toegewezen, of om de taken van algemeen belang te vervullen die door of krachtens een wet, een decreet of een ordonnantie aan hen

zijn toevertrouwd. De VKBO is complementair aan de Kruispuntbank van Ondernemingen. De VKBO bezorgt systematisch aan de Kruispuntbank van Ondernemingen en de respectieve gegevensbronnen alle ontvangen meldingen over onnauwkeurige, onvolledige of onjuiste gegevens;

12° indien nodig, alfanumerieke gegevens verzamelen en elektronisch opslaan, beheren en verwerken om ter beschikking te stellen aan de instanties en externe overheden die de gegevens nodig hebben om onderzoeken en opdrachten uit te voeren die hun door of krachtens een wet, een decreet of een ordonnantie zijn toegewezen, of om de taken van algemeen belang te vervullen die door of krachtens een wet, een decreet of een ordonnantie aan hen zijn toevertrouwd;

13° samenwerking met andere dienstenintegratoren organiseren;

14° gegevens verzamelen, samenvoegen, coderen of anonimiseren en ter beschikking stellen, als intermediaire organisatie als vermeld in 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. De VDI mag de persoonsgegevens die verwerkt worden in het kader van deze opdracht, alleen bijhouden zolang dat noodzakelijk is om ze te coderen of te anonimiseren. De VDI mag evenwel het verband tussen het reële identificatienummer van een persoon en het aan hem toegekend gecodeerd identificatienummer bijhouden als de bestemming van de gecodeerde persoonsgegevens daarom verzoekt op een gemotiveerde wijze, na machtiging van de Vlaamse toezichtcommissie of een sectoraal comité binnen de Commissie voor de bescherming van de persoonlijke levenssfeer;

15° de naleving van de visie, de strategie, de functionele en technische normen, standaarden en specificaties, de basisarchitectuur, alsook het gebruik van het gegevensuitwisselingsplatform voor de veilige elektronische gegevensuitwisseling en de basisdiensten en de verwezenlijking van de programma's en de projecten door zoveel mogelijk instanties bevorderen.

**Art. 5.** De VDI heeft, in permanente afstemming met de instanties en de andere dienstenintegratoren, in het bijzonder als opdracht de integratie van gegevensverwerkende processen, en in dat kader de geïntegreerde ontsluiting van gegevens. Daarvoor is de VDI ermee belast :

1° de aanvragen tot raadpleging van de gegevens, opgenomen in een of meer gegevensbronnen, en de aanvragen tot mededeling van de gegevens, opgenomen in een of meer gegevensbronnen, te ontvangen en er gevolg aan te geven, of die gegevens geïntegreerd mee te delen;

2° de wijzen uit te werken waarop de toegangsrechten tot de gegevensbronnen door de VDI technisch en organisatorisch kunnen worden gecontroleerd;

3° de homogeniteit van de toegangsrechten tot de gegevensbronnen te bevorderen en te bewaken;

4° de technische voorwaarden, goedgekeurd door het coördinatiecomité, vermeld in artikel 20, uit te werken en in te voeren om de toegangskanalen zo efficiënt en veilig mogelijk uit te bouwen;

5° de technische voorwaarden, goedgekeurd door het coördinatiecomité, vermeld in artikel 20, voor de communicatie tussen de gegevensbronnen of tussen de authentieke gegevensbronnen en de instanties uit te werken en in te voeren;

6° een gecoördineerd veiligheidsbeleid te bevorderen;

7° de diensten van de VDI kenbaar te maken bij de instanties, externe overheden en andere dienstenintegratoren;

8° de omvorming van gegevensbronnen tot authentieke gegevensbronnen te bevorderen en te begeleiden.

**Art. 6. § 1.** Bij de verwerking van gegevens met toepassing van dit decreet en de uitvoeringsbesluiten ervan worden uitsluitend de volgende identificatiemiddelen gebruikt :

1° het identificatienummer van het Rijksregister, als de gegevens betrekking hebben op een natuurlijke persoon die in het Rijksregister opgenomen is;

2° het identificatienummer van de Kruispuntbank van de Sociale Zekerheid, als de gegevens betrekking hebben op een natuurlijk persoon die niet in het Rijksregister is opgenomen;

3° het ondernemingsnummer, als de gegevens betrekking hebben op een onderneming die is opgenomen in de Kruispuntbank van Ondernemingen;

4° de identificator, vermeld in artikel 2, 9°, van het decreet van 8 mei 2009 betreffende het Centraal Referentieadressenbestand, als de gegevens betrekking hebben op adressen als vermeld in artikel 6 van het decreet van 8 mei 2009 betreffende het Centraal Referentieadressenbestand;

5° het kadastraal perceelsnummer, als de gegevens betrekking hebben op percelen;

6° de identificatoren van de geografische objecten van het Grootchalig Referentie Bestand, vermeld in punt 4.3 van de bijlage bij het ministerieel besluit van 11 maart 2005 houdende goedkeuring van de GRB-specificaties in uitvoering van het decreet van 16 april 2004 houdende het Grootchalig Referentie Bestand, als de gegevens betrekking hebben op of verwijzen naar exemplaren van het GRB.

§ 2. Voor de gegevens die niet onder de toepassing van paragraaf 1 vallen, kan de Vlaamse Regering het gebruik van andere identificatiemiddelen opleggen.

**Art. 7. § 1.** De instanties delen aan de VDI langs elektronische weg alle elektronisch beschikbare gegevens mee die hij nodig heeft om zijn opdracht als dienstenintegrator uit te voeren.

§ 2. De VDI deelt aan de instanties, externe overheden en de andere dienstenintegratoren langs elektronische weg alle elektronisch beschikbare gegevens mee die deze nodig hebben om hun opdrachten uit te voeren.

§ 3. Voor elke elektronische mededeling van persoonsgegevens door of aan de VDI is een machtiging vereist, tenzij die elektronische mededeling bij of krachtens een wettelijke of decretale bepaling is toegestaan of is vrijgesteld van een machtiging, telkens na advies van de Vlaamse toezichtcommissie of van het bevoegde sectoraal comité.

§ 4. Een elektronische mededeling van persoonsgegevens kan pas plaatsvinden nadat de machtiging, vermeld in paragraaf 3, is verleend en als de voorwaarden en de nadere regels nageleefd worden die in voorkomend geval door de Vlaamse toezichtcommissie of het sectoraal comité voor de mededeling in de machtiging zijn bepaald.

**Art. 8.** De VDI onderzoekt bij elk verzoek tot raadpleging of mededeling van gegevens of de aanvrager en het betreffende verzoek voldoen aan de specifieke regels inzake de voorwaarden voor raadpleging of mededeling van bepaalde gegevens voor de desbetreffende gegevensbron of voor de authentieke gegevensbron, vastgelegd door de betreffende gegevensbron of door de authentieke gegevensbron.

**Art. 9.** Het beroep doen op de VDI mag er op geen enkele wijze toe leiden dat een aanvrager gegevens kan raadplegen of dat gegevens aan hem worden meegedeeld die hij niet zou kunnen verkrijgen via de rechtstreekse raadpleging van de afzonderlijke gegevensbronnen of authentieke gegevensbronnen, rekening houdend met de wettelijke, decretale en reglementaire bepalingen die op die gegevens van toepassing zijn.

**Art. 10.** De VDI kan, in permanente afstemming met de instanties, voorzien in functies die leiden tot de integratie van diensten, aangeboden door een of meer gegevensbronnen of authentieke gegevensbronnen.

**Art. 11.** § 1. Functies die leiden tot de integratie van diensten, aangeboden door een of meer gegevensbronnen of authentieke gegevensbronnen, mogen er op geen enkele wijze toe leiden dat een aanvrager informatie verkrijgt die hij, rekening houdend met de wettelijke, decretale en reglementaire bepalingen, niet mag verkrijgen.

§ 2. Functies die leiden tot de integratie van diensten, kunnen gebruikmaken van gegevens die de aanvrager op zich niet mag raadplegen of die aan hem niet meegedeeld mogen worden, als :

1° de specifieke regels inzake de voorwaarden voor raadpleging of mededeling van bepaalde gegevens voor de desbetreffende gegevensbron of authentieke gegevensbron dat uitdrukkelijk toestaan;

2° het integratieresultaat niet toelaat om expliciet of impliciet gegevens of informatie te verkrijgen of af te leiden die de aanvrager ingevolge paragraaf 1 niet mag verkrijgen;

3° het gebruik van dergelijke gegevens noodzakelijk is om tot het integratieresultaat te komen.

**Art. 12.** De VDI voorziet in gepaste middelen waarmee een aanvrager in eigen naam of voor rekening van een andere persoon inzage in zijn gegevens kan krijgen of zijn gegevens meegedeeld kan krijgen via de VDI.

**Art. 13.** De via de VDI elektronisch meegedeelde gegevens, alsook de weergave ervan op een leesbare drager, genieten, tot bewijs van het tegendeel, dezelfde wettelijke bewijswaarde als wanneer ze op papieren drager zouden zijn meegedeeld.

#### HOOFDSTUK 4. — Verwerking van persoonsgegevens

**Art. 14.** Dit decreet doet op geen enkele wijze afbreuk aan de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens of aan bijzondere wettelijke, decretale of reglementaire bepalingen over de bescherming van gegevens en persoonsgegevens die van toepassing zijn op bepaalde gegevensbronnen.

**Art. 15.** § 1. De VDI staat in voor de wijze waarop en de mate waarin het recht om gegevens die via de VDI worden verwerkt, kosteloos te laten verbeteren, kan worden uitgeoefend, zoals dat, voor de verbetering van persoonsgegevens, bepaald is in artikel 12 van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.

Verzoeken tot aanpassing van onnauwkeurige, onvolledige of onjuiste gegevens kunnen worden ingediend via de toegangskanalen, bepaald door de VDI en de betrokken instanties. De VDI en de betrokken instanties leggen vast op welke manier de verzoeken worden onderzocht, op welke wijze het resultaat van het onderzoek aan de verzoeker wordt meegedeeld en hoe aan het resultaat gevolg wordt gegeven.

§ 2. Elke persoon heeft het recht om te weten welke instanties en externe overheden, gedurende de laatste zes maanden persoonsgegevens over hem via de VDI hebben geraadpleegd of bijgewerkt, met uitzondering van de bestuurlijke en gerechtelijke instanties die belast zijn met de opsporing en bestraffing van misdrijven, alsook van de Veiligheid van de Staat en de Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht.

De VDI voorziet daartoe in de gepaste middelen overeenkomstig de voorwaarden en regels, bepaald door de Vlaamse toezichtcommissie.

#### HOOFDSTUK 5. — Vertrouwelijkheidsverplichting

**Art. 16.** Elke persoon die uit hoofde van zijn functie betrokken is bij de inzameling, raadpleging, mededeling, bij het gebruik of bij een andere verwerking van gegevens die krachtens wettelijke, decretale of reglementaire bepalingen onder een beroepsgeheim vallen, is ertoe gehouden het vertrouwelijke karakter van die gegevens te eerbiedigen alsof hij zelf onderworpen is aan dat beroepsgeheim. Die persoon wordt evenwel van die plicht ontheven als hij geroepen wordt om in rechte getuigenis af te leggen, als hij bij of krachtens de wet of het decreet van die plicht is ontslagen, als hij verplicht is bekend te maken wat hij weet of nadat hij het schriftelijke akkoord heeft gekregen van de derde die door de onthulling zal worden getroffen.

**Art. 17.** Elke persoon die uit hoofde van zijn functie betrokken is bij de inzameling, raadpleging, mededeling, bij het gebruik of bij een andere verwerking van gegevens via de VDI, is ertoe gehouden het vertrouwelijke karakter van de gegevens te bewaren. Elke schending van de vertrouwelijkheidsverplichting wordt gestraft met een gevangenisstraf van acht dagen tot zes maanden en met een geldboete van honderd euro tot vijfhonderd euro.

#### HOOFDSTUK 6. — Vernietiging van gegevensbronnen

**Art. 18.** De Vlaamse Regering wijst de personen aan die in oorlogstijd, in omstandigheden die daarmee gelijkgesteld zijn krachtens artikel 7 van de wet van 12 mei 1927 op de militaire opeisingen, of tijdens de bezetting van het grondgebied door de vijand ermee belast zijn om de toegang tot de gegevens en de gegevensbronnen bij de VDI te verhinderen of om de gegevensbronnen geheel of gedeeltelijk te vernietigen of te laten vernietigen. De Vlaamse Regering bepaalt de verhindering van de toegang of de vernietiging nader.

#### HOOFDSTUK 7. - Veiligheidsconsulent

**Art. 19.** § 1. De VDI wijst, onder zijn personeel en na advies van de Vlaamse toezichtcommissie, een veiligheidsconsulent aan als vermeld in het besluit van de Vlaamse Regering van 15 mei 2009 betreffende de veiligheidsconsulenten.

§ 2. De veiligheidsconsulent van de VDI voert, met het oog op de veiligheid van de gegevens die door de VDI worden verwerkt of uitgewisseld en met het oog op de bescherming van de persoonlijke levenssfeer van de personen op wie de gegevens betrekking hebben, zijn opdrachten uit overeenkomstig het besluit van de Vlaamse Regering van 15 mei 2009 betreffende de veiligheidsconsulenten.

Onverminderd de opdrachten, vermeld in het besluit van de Vlaamse Regering van 15 mei 2009 betreffende de veiligheidsconsulenten, werkt de veiligheidsconsulent samen met de veiligheidsconsulenten van de andere instanties, externe overheden en dienstenintegratoren om te komen tot een coherente benadering van informatiebeveiliging. De veiligheidsconsulent van de VDI zorgt ook voor de sensibilisering van de informatiebeveiliging bij de instanties in kwestie. De Vlaamse Regering kan aan de veiligheidsconsulent van de VDI nog bijkomende opdrachten opleggen.

De naleving van de veiligheidsvereisten, zoals bepaald in artikel 16 van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, door de VDI en de gebruikers van de VDI wordt jaarlijks geevalueerd door de Vlaamse toezichtcommissie.

#### HOOFDSTUK 8. — Het coördinatiecomité

**Art. 20.** Bij de VDI wordt een coördinatiecomité opgericht dat bestaat uit vertegenwoordigers van de instanties en van de provinciale en lokale besturen. Alle Vlaamse dienstenintegratoren maken ook deel uit van het coördinatiecomité.

Het coördinatiecomité staat de VDI bij in de vervulling van zijn opdrachten. Daartoe stelt het coördinatiecomité initiatieven voor ter bevordering en ter bestendiging van elektronische dienstverlening aan de instanties en externe overheden, en stelt alle nuttige maatregelen voor die kunnen bijdragen tot een veilige en vertrouwelijke behandeling van persoonsgegevens of tot een administratieve vereenvoudiging voor de instanties in kwestie.

Het coördinatiecomité kan intern werkgroepen oprichten waaraan het bijzondere taken toevertrouwt. Het stelt zijn huishoudelijk reglement op en legt het ter goedkeuring voor aan de Vlaamse Regering.

**Art. 21.** Het coördinatiecomité brengt aan de VDI advies uit over :

- 1° de mogelijke ontsluiting via de VDI van gegevensbronnen of authentieke gegevensbronnen;
- 2° de mogelijke aanpassing van de gegevensbronnen zodat, als dat mogelijk is, alleen authentieke gegevens worden ontsloten;
- 3° de optimalisering binnen de instanties van de aanmaak, het gebruik, de uitwisseling en het beheer van gegevensbronnen en authentieke gegevensbronnen;
- 4° een gestructureerde aanpak bij de uitbouw van een stelsel van Vlaamse authentieke gegevensbronnen, met inbegrip van het promoten, begeleiden en coördineren van authentieke gegevensbronnen bij de instanties;
- 5° het gebruik van verwijzingen naar het gegeven in de gegevensbron of de authentieke gegevensbron voor gegevens die geheel of gedeeltelijk overlappen met een authentiek gegeven in een authentieke gegevensbron;
- 6° het vastleggen van regels voor de gegevensbron of de authentieke gegevensbron inzake de voorwaarden voor raadpleging door of mededeling aan een verzoekende instantie van bepaalde gegevens.

Het coördinatiecomité beraadslaagt over initiatieven ter bevordering en ter bestendiging van de samenwerking inzake elektronisch gegevensverkeer en over initiatieven die kunnen bijdragen tot een rechtmatige en vertrouwelijke behandeling van de gegevens.

Het coördinatiecomité kan ook adviezen verstrekken of aanbevelingen formuleren over informatisering en elektronisch bestuurlijk gegevensverkeer of aanverwante materies, voorstellen doen voor of meewerken aan de organisatie van opleidingscursussen over informatica en elektronisch bestuurlijk gegevensverkeer voor het personeel van de instanties en onderzoeken hoe de rationele uitwisseling van gegevens kan worden bevorderd.

Het coördinatiecomité beraadslaagt uit eigen beweging of op verzoek van de Vlaamse Regering, een lid van de Vlaamse Regering, de VDI of een instantie. De Vlaamse Regering kan bepalen in welke gevallen de raadpleging van het coördinatiecomité verplicht is.

De leden van het coördinatiecomité streven consensus na. Als geen consensus wordt bereikt, geeft het coördinatiecomité in het advies en in de beraadslaging de verschillende standpunten weer.

**Art. 22.** Het coördinatiecomité wordt minstens jaarlijks bijeengeroepen op initiatief van de voorzitter of telkens als een van de leden van het coördinatiecomité daarom verzoekt.

De Vlaamse Regering stelt de samenstelling van het coördinatiecomité vast, bepaalt de samenstelling en de werking van het secretariaat dat belast is met de administratieve ondersteuning en de organisatie van het coördinatiecomité, omschrijft, zo nodig, nader zijn bevoegdheden, bepaalt de nadere regels voor de werking en benoemt de voorzitter en de leden.

De VDI draagt de werkingskosten van het coördinatiecomité en van de werkgroepen die erin worden opgericht.

#### HOOFDSTUK 9. — Wijzigings- en slotbepalingen

**Art. 23.** In het decreet van 22 december 2006 houdende bepalingen tot begeleiding van de begroting 2007, gewijzigd bij de decreten van 21 december 2007, 19 december 2008 en 23 december 2010, worden de volgende wijzigingen aangebracht :

- 1° het opschrift van hoofdstuk XXIII wordt vervangen door wat volgt : "Hoofdstuk XXIII. DAB Informatie Vlaanderen";
- 2° in artikel 79, § 1, worden de woorden "ICT (DAB ICT)" vervangen door de woorden "Informatie Vlaanderen";
- 3° in artikel 79, § 2, worden de woorden "DAB ICT" vervangen door de woorden "DAB Informatie Vlaanderen";
- 4° in artikel 79, § 2bis, ingevoegd bij het decreet van 19 december 2008, worden de volgende wijzigingen aangebracht :
  - a) de woorden "DAB ICT" worden vervangen door de woorden "DAB Informatie Vlaanderen";
  - b) aan het tweede lid wordt een zin toegevoegd, die luidt als volgt : "Hij vervult de functie van dienstenintegrator overeenkomstig het decreet houdende de oprichting en organisatie van een Vlaamse dienstenintegrator. » ;
- 5° in artikel 79, § 3, worden de woorden "DAB ICT" telkens vervangen door de woorden "DAB Informatie Vlaanderen".

**Art. 24.** In artikel 2, 15°, van het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer worden de volgende wijzigingen aangebracht :

- 1° de woorden "Vlaamse overheid" worden vervangen door de woorden "entiteiten van de Vlaamse administratie of de provinciale en lokale besturen";
- 2° tussen het woord "van" en het woord "regelgeving" wordt het woord "Vlaamse" ingevoegd.

**Art. 25.** In hetzelfde decreet wordt afdeling II van hoofdstuk II, die bestaat uit artikel 5, opgeheven.

**Art. 26.** De Vlaamse Regering brengt twee jaar na de inwerkingtreding van dit decreet aan het Vlaams Parlement verslag uit over de toepassing van dit decreet, in voorkomend geval met toevoeging van aanbevelingen die kunnen leiden tot een decretaal initiatief of tot andere maatregelen voor een passende uitvoering van dit decreet. Het verslag is gebaseerd op een evaluatieverslag van de VDI zelf, een evaluatieverslag van de Vlaamse toezichtcommissie en een verslag van het coördinatiecomité, vermeld in artikel 20.

**Art. 27.** Dit decreet treedt in werking op de dag van de bekendmaking ervan in het *Belgisch Staatsblad*.

Kondigen dit decreet af, bevelen dat het in het *Belgisch Staatsblad* zal worden bekendgemaakt.

Brussel, 13 juli 2012.

De minister-president van de Vlaamse Regering,  
K. PEETERS

De Vlaamse minister van Bestuurszaken, Binnenlands Bestuur, Inburgering, Toerisme en Vlaamse Rand,  
G. BOURGEOIS

Nota

(1) *Zitting 2011-2012.*

*Stukken.* — Ontwerp van decreet, 1516 - Nr. 1. — Verslag, 1516 - Nr. 2. — Tekst aangenomen door de plenaire vergadering, 1516 - Nr. 3.

*Handelingen.* — Bespreking en aanneming. Ochtend- en avondvergadering van 4 juli 2012.

## TRADUCTION

### AUTORITE FLAMANDE

F. 2012 — 2234

[C - 2012/35894]

#### 13 JUILLET 2012. — Décret portant création et organisation d'un intégrateur de services flamand (1)

Le PARLEMENT FLAMAND a adopté et Nous, GOUVERNEMENT, sanctionnons ce qui suit :

Décret relatif à la création et à l'organisation d'un intégrateur de services flamand.

#### CHAPITRE 1<sup>er</sup>. — Dispositions générales

**Article 1<sup>er</sup>.** Le présent décret règle une matière communautaire et régionale.

**Art. 2.** Dans le présent décret, on entend par :

1° source de données authentique : une source de données authentique telle que visée à l'article 4, § 1<sup>er</sup> et § 2, du décret du 18 juillet 2008 relatif à l'échange électronique de données administratives;

2° La commission de contrôle flamande : la commission de contrôle flamande, instituée par l'article 10 du décret du 18 juillet 2008 relatif à l'échange électronique de données administratives;

3° intégrateur de services une instance qui par ou en vertu d'une loi, d'un décret ou d'une ordonnance est chargée, au sein d'un niveau déterminé de l'administration ou dans un secteur déterminé, d'une tâche d'intérêt général et, plus précisément, de l'organisation de l'échange électronique de données entre différentes instances et de l'accès intégré aux données;

4° autorité externe : une autorité appartenant au niveau international ou fédéral, une autre communauté ou région, et les institutions ou personnes morales qui en relèvent, ainsi que les personnes morales de droit privé qui sont chargées de tâches ou missions d'intérêt général;

5° l'arrêté du Gouvernement flamand du 15 mai 2009 relatif aux conseillers en sécurité : l'arrêté du Gouvernement flamand du 15 mai 2009 relatif aux conseillers en sécurité, mentionné à l'article 9 du décret du 18 juillet 2008;

6° instances : les instances visées à l'article 4, § 1<sup>er</sup>, du décret du 26 mars 2004 relatif à la publicité de l'administration;

7° autorisation : l'autorisation, mentionnée à l'article 8 du décret du 18 juillet 2008 relatif à l'échange électronique de données administratives, accordée par la commission de contrôle flamande ou un comité sectoriel compétent selon que la communication électronique de données à caractère personnel requiert une autorisation de la commission flamande de contrôle ou d'un comité sectoriel;

8° comité sectoriel : un comité sectoriel, institué au sein de la Commission pour la protection de la vie privée conformément à l'article 31 bis de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel;

9° ISF : l'intégrateur de services flamand.

#### CHAPITRE 2. — Création de l'ISF

**Art. 3. § 1<sup>er</sup>.** Le DAB Informatie Vlaanderen (SGC Information Flandres), visé à l'article 79 du décret du 22 décembre 2006 contenant diverses mesures d'accompagnement du budget 2007, remplit la fonction d'intégrateur de services dans le but de simplifier et d'optimiser les échanges de données mutuels entre les instances, d'une part, et entre les instances et les autres intégrateurs de services et autorités externes, d'autre part.

L'ISF soutient les instances en organisant des prestations de services électroniques mutuelles et des échanges électroniques de données entre les instances entre elles, entre les instances et les autorités externes et entre les instances et les autres intégrateurs de services afin de permettre aux instances d'exécuter les missions pour les utilisateurs des services qu'elles proposent, de manière effective et efficace, moyennant un minimum de charges et de frais administratifs. La collecte unique et un accès coordonné aux données sont centraux dans le fonctionnement de l'ISF.

L'ISF organise les prestations de services électroniques et l'échange électronique de données avec des garanties sur le plan de la sécurité de l'information et de la protection de la vie privée et ce, en étroite concertation avec les instances, autorités externes et les autres intégrateurs de services.

§ 2. En dérogation au paragraphe 1, l'ISF ne soutient pas les prestations de services électroniques et l'échange électronique de données qui sont assurés par un autre intégrateur de services par ou en vertu de la loi, d'un décret ou d'une ordonnance.

L'ISF canalise, en accord avec d'autres intégrateurs de services, l'échange de données tel que visé au paragraphe 1.

§ 3. A défaut de dispositions décrétales ou réglementaires autres, l'ISF n'accorde aucunement, à des personnes ou instances, des droits complémentaires de consultation, de communication ou de tout autre traitement de données en plus des dispositions décrétales et réglementaires applicables.

### CHAPITRE 3. — Missions et fonctionnement de l'ISF

**Art. 4.** Pour l'exécution de son but, l'ISF est chargé des missions suivantes :

1° développer une vision et une stratégie en vue de prestations de services électroniques et d'un échange électronique de données effectifs, efficaces et dûment protégés, tels que visés à l'article 3, et en surveiller le respect;

2° promouvoir et surveiller l'homogénéité et la cohérence de la politique à l'aide de la stratégie, visée au point 1°;

3° concevoir, développer et gérer une plateforme centrale d'échange de données, qui se compose de services et d'une infrastructure ICT génériques et qui permet, de manière générique, l'échange de données entre les différentes sources de données. Cette plateforme est gérée par des instances ou autorités externes;

4° concevoir, développer et mettre à disposition des services de base utiles afin de soutenir l'échange électronique de données, par exemple un système pour l'organisation et le logging des échanges électroniques de données, un système d'accès électronique aux données, un système pour utilisateurs et gestion de l'accès, un système de datage électronique et un système de codage et d'anonymisation des informations;

5° établir des accords clairs, sur la base d'une répartition des tâches, entre les parties concernées concernant les points suivants :

a) qui effectue quels authentications, vérifications et contrôles, à l'aide de quels moyens, et qui en assume la responsabilité;

b) la manière dont les résultats des authentications, les vérifications et les contrôles exécutés font l'objet d'un échange et d'une conservation électroniques sécurisés entre les parties concernées;

c) qui tient à jour des loggings déterminés;

d) la manière dont on veille, dans le cadre d'un examen, à l'initiative d'une partie concernée ou d'un organe de contrôle concerné ou à la suite d'une plainte, à ce qu'une reconstruction complète puisse avoir lieu concernant quelle personne physique a utilisé un service ou une transaction déterminés concernant un citoyen ou une entreprise déterminés et quand, par le biais de quel canal et à quelles fins;

6° conformément à la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, gérer un répertoire de références indiquant les instances auprès desquelles des types déterminés de données sont conservés concernant des personnes, entreprises ou institutions déterminés ou qui fait référence à la source de données où ces données peuvent être consultées ou qui, par personne physique ou entreprise, indique quels types de données sont mis à disposition d'instances ou d'autorités externes déterminées et pour quelle période, avec mention du but pour lequel l'instance ou l'autorité externe a besoin de ces données et gérer un répertoire d'autorisations qui stipule qui a accès, sous quelles conditions, à des données déterminées. L'implémentation du répertoire de références et d'autorisations ne pourra être réalisée qu'après avis de la commission de contrôle flamande;

7° encadrer les instances lors de la mise en œuvre de la stratégie visée au point 1°;

8° développer et introduire des normes, standard, spécifications TIC fonctionnels et techniques ainsi qu'une architecture de base qui ont été approuvés par le comité de coordination, visé à l'article 20, afin d'utiliser la TIC de manière efficace à l'appui de la vision et de la stratégie, visées au point 1°, et en vue d'en surveiller le respect;

9° gérer et coordonner les aspects TIC organisationnels, fonctionnels et techniques de l'échange de données;

10° élaborer des programmes, projets et services qui regroupent potentiellement les instances et qui soutiennent la stratégie commune, visée au point 1°;

11° gérer la Banque-Carrefour enrichie des entreprises, abrégée en BCEE. La BCEE est une source de données où sont enregistrées des données d'identification d'entreprises provenant de la Banque-Carrefour des Entreprises et enrichie de données d'entreprises provenant de différentes sources de données gérées par d'autres instances et autorités externes. Les données enregistrées dans la BCEE sont mises à disposition des instances et autorités externes afin d'exécuter les missions qui leur ont été attribuées par ou en vertu d'une loi, d'un décret ou d'une ordonnance ou pour remplir les tâches d'intérêt général qui leur ont été confiées par ou en vertu d'une loi, d'un décret ou d'une ordonnance. La BCEE est complémentaire à la Banque-Carrefour des Entreprises. La BCEE fournit systématiquement à la Banque-Carrefour des Entreprises et aux sources de données respectives toutes les notifications reçues concernant des données imprécises, incomplètes ou erronées;

12° rassembler et enregistrer électroniquement, au besoin, des données alphanumériques, les gérer et les traiter afin de mettre à la disposition des instances et autorités externes qui ont besoin des données en vue d'exécuter des examens et missions qui leur ont été attribués par ou en vertu d'une loi, d'un décret ou d'une ordonnance ou pour remplir les tâches d'intérêt général qui leur ont été confiées par ou en vertu d'une loi, d'un décret ou d'une ordonnance.

13° organiser la collaboration avec d'autres intégrateurs de services;

14° en tant qu'organisme intermédiaire tel que visé à l'Arrêté Royal du 13 février 2001, portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, recueillir, agréger, coder ou anonymiser et mettre à disposition des données; L'ISF ne pourra conserver les données à caractère personnel traitées dans le cadre de cette mission que pour la durée nécessaire à leur codification ou anonymisation; L'ISF peut cependant conserver le lien entre le numéro d'identification réel d'une personne concernée et le numéro d'identification codé qui lui a été attribué si le destinataire des données à caractère personnel codées en fait la demande d'une façon motivée, moyennant une autorisation de la commission de contrôle flamande ou d'un comité sectoriel au sein de la Commission pour la protection de la vie privée;

15° promouvoir le respect de la vision, de la stratégie, des normes, standard et spécifications fonctionnels et techniques, de l'architecture de base ainsi que l'utilisation de la plateforme d'échange de données pour l'échange électronique de données sécurisé et des services de base et la réalisation des programmes et projets par un maximum d'instances.

**Art. 5.** L'ISF a, en accord permanent avec les instances et autres intégrateurs de services, comme mission particulière de réaliser l'intégration de processus de traitement de données et, dans ce cadre, l'accès intégré aux données. Pour ce faire, l'ISF est chargé :

1° de recevoir les demandes de consultation des données, enregistrées dans une ou plusieurs sources de données, et les demandes de communication de données, enregistrées dans une ou plusieurs sources de données et d'y donner suite ou de communiquer ces données de manière intégrée;

2° d'élaborer les modes de contrôle technique et organisationnel, par l'ISF, des droits d'accès aux sources de données;

3° de promouvoir et de surveiller l'homogénéité des droits d'accès aux sources de données;

4° d'élaborer et d'introduire les conditions techniques, approuvées par le comité de coordination, mentionné à l'article 20, afin d'ainsi développer les canaux d'accès de la manière la plus efficace et la plus sûre possible;

5° d'élaborer et d'introduire les conditions techniques, approuvées par le comité de coordination, visé à l'article 20, pour la communication entre les sources de données ou entre les sources de données authentiques et les instances;

6° de promouvoir la coordination de la politique de sécurité;

7° d'informer les instances, autorités externes et autres intégrateurs de services des services de l'ISF;

8° de favoriser et d'accompagner la transformation de sources de données en sources de données authentiques.

**Art. 6.** § 1<sup>er</sup>. Pour le traitement des données en application du présent décret et de ses arrêtés d'exécution, seuls les moyens d'identification suivants seront utilisés :

1° le numéro d'identification du Registre national lorsque les données ont trait à une personne physique reprise dans le Registre national;

2° le numéro d'identification de la Banque-Carrefour de la Sécurité sociale lorsque les données ont trait à une personne physique qui n'est pas reprise dans le Registre national;

3° le numéro d'entreprise lorsque les données ont trait à une entreprise enregistrée à la Banque-Carrefour des Entreprises;

4° l'identificateur, visé à l'article 2, 9°, du décret du 8 mai 2009 relatif au Fichier central d'Adresses de Référence lorsque les données ont trait à des adresses mentionnées à l'article 6 du décret du 8 mai 2009 concernant le Fichier central d'Adresses de Référence;

5° le numéro cadastral de parcelle lorsque les données ont trait à des parcelles;

6° les identificateurs des objets géographiques du «Grootschalig Referentie Bestand (Base de données des références à grande échelle), mentionné au point 4.3 de l'annexe à l'arrêté ministériel du 11 mars 2005 portant approbation des spécifications GRB en exécution du décret du 16 avril 2004 relatif au «Grootschalig Referentie Bestand » lorsque les données ont trait ou font référence à des exemplaires du GRB.

§ 2. Pour les données qui ne relèvent pas de l'application du paragraphe 1, le Gouvernement flamand peut imposer l'utilisation d'autres moyens d'identification.

**Art. 7.** § 1<sup>er</sup>. Les instances communiquent à l'ISD, par voie électronique, toutes les données électroniquement disponibles dont il a besoin pour exécuter sa mission en qualité d'intégrateur de services.

§ 2. L'ISF communique aux instances, aux autorités externes et aux autres intégrateurs de services, par voie électronique, toutes les données électroniquement disponibles dont ceux-ci ont besoin pour exécuter leurs missions.

§ 3. Toute communication électronique de données à caractère personnel par l'ISF ou à l'ISF requiert une autorisation, à moins que cette communication électronique ne soit autorisée ou soit exemptée d'autorisation par ou en vertu d'une disposition légale ou décrétole, chaque fois après avis de la commission de contrôle flamande ou du comité sectoriel compétent.



§ 4. Une communication électronique de données à caractère personnel ne peut avoir lieu qu'après que l'autorisation, visée au paragraphe 3, a été accordée et si les conditions et les autres modalités sont respectées telles qu'elles ont été fixées le cas échéant par la commission de contrôle flamande ou le comité sectoriel pour la communication dans l'autorisation.

**Art. 8.** L'ISF examine, pour chaque requête de consultation ou de communication de données, si le demandeur et la requête concernée satisfont aux règles spécifiques relatives aux conditions d'application à la consultation ou à la communication de données déterminées pour la source de données concernée ou pour la source de données authentique comme fixées par la source de données concernée ou la source de données authentiques.

**Art. 9.** Le recours à l'ISF ne confère en aucune manière à un demandeur le droit de consulter ou de se voir communiquer des données qu'il ne pourrait pas obtenir en consultant directement les sources de données distinctes ou des sources de données authentiques, compte tenu des dispositions légales, décrétales et réglementaires applicables aux données en question.

**Art. 10.** En accord permanent avec les instances, l'ISF peut pourvoir à des fonctions qui débouchent sur l'intégration de services proposés par une ou plusieurs sources de données ou sources de données authentiques.

**Art. 11.** § 1<sup>er</sup>. Les fonctions qui débouchent sur l'intégration de services proposés par une ou plusieurs sources de données ou sources de données authentiques ne peuvent en aucune manière avoir pour effet que le demandeur reçoit des informations qu'il n'est pas en droit d'obtenir compte tenu des dispositions légales, décrétales et réglementaires.

§ 2. Les fonctions qui débouchent sur l'intégration de services peuvent utiliser des données que le demandeur en soi ne peut pas consulter ou qui ne peuvent pas lui être communiquées si :

1° les règles spécifiques relatives aux conditions de consultation ou de communication de certaines données pour la source de données concernée ou la source de données authentique le permettent expressément;

2° le résultat d'intégration ne permet pas d'obtenir, explicitement ou implicitement, des données ou informations que le demandeur n'est pas en droit d'obtenir conformément au paragraphe 1 ou de les déduire;

3° l'utilisation de telles données est nécessaire pour arriver au résultat d'intégration.

**Art. 12.** L'ISF prévoit des moyens appropriés permettant à un demandeur de pouvoir consulter ses données ou de se voir communiquer des données par le biais de l'ISF, en son nom propre ou pour le compte d'une autre personne.

**Art. 13.** Les données communiquées par voie électronique par le biais de l'ISF, ainsi que leur reproduction sur un support lisible, ont, jusqu'à preuve du contraire, la même valeur probante légale que si elles avaient été communiquées sur support papier.

#### CHAPITRE 4. — Traitement des données à caractère personnel

**Art. 14.** Le présent décret ne porte nullement atteinte à la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel ou aux dispositions légales, décrétales ou réglementaires particulières relatives à la protection de données et de données à caractère personnel applicables à des sources de données déterminées.

**Art. 15.** § 1<sup>er</sup>. L'ISF garantit la façon dont et la mesure dans laquelle le droit à faire corriger gratuitement les données qui sont traitées par le biais de l'ISF peut être exercé conformément aux dispositions d'application à la correction de données à caractère personnel fixées à l'article 12 de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

Les demandes d'adaptation de données imprécises, incomplètes ou erronées peuvent être introduites par le biais des canaux d'accès fixés par l'ISF et les instances concernées. L'ISF et les instances concernées déterminent de quelle manière les demandes sont examinées, de quelle façon le résultat de l'examen est communiqué au demandeur et la façon dont il est donné suite au résultat.

§ 2. Toute personne a le droit de savoir quelles instances et autorités externes ont, au cours des six mois écoulés, consulté ou mis à jour des données à caractère personnel la concernant, par le biais de l'ISF, à l'exception des autorités administratives et judiciaires chargées de la recherche et de la répression de délits, de même que de la Sûreté de l'Etat et du Service Général du Renseignement et de la Sécurité des Forces Armées.

L'ISF prévoit à cet effet les moyens appropriés conformément aux conditions et règles fixées par la Commission de contrôle flamande.

#### CHAPITRE 5. — Obligation de confidentialité

**Art. 16.** Toute personne qui, en raison de ses fonctions, participe à la collecte, à la consultation, à la communication, à l'utilisation ou à tout autre traitement de données qui sont couvertes par le secret professionnel en vertu de dispositions légales, décrétales ou réglementaires, est tenue d'observer le caractère confidentiel de ces données comme si elle était elle-même soumise à ce secret professionnel. La personne en question est toutefois libérée de cette obligation lorsqu'elle est appelée à témoigner en justice, si la loi ou le décret la dispense de cette obligation, si elle est obligée de faire connaître ce qu'elle sait ou après avoir obtenu l'accord écrit du tiers qui sera concerné par la divulgation.

**Art. 17.** Toute personne qui, en raison de ses fonctions, participe à la collecte, à la consultation, à la communication, à l'utilisation ou à tout autre traitement de données par le biais de l'ISF s'engage à maintenir le caractère confidentiel des données. Toute violation de l'obligation de confidentialité sera sanctionnée d'une peine d'emprisonnement de huit jours à six mois et d'une amende de cent euros à cinq cents euros.

## CHAPITRE 6. — Destruction de sources de données

**Art. 18.** Le Gouvernement flamand désigne les personnes qui, en temps de guerre, dans des circonstances y assimilées en vertu de l'article 7 de la loi du 12 mai 1927 sur les réquisitions militaires ou pendant l'occupation du territoire par l'ennemi sont chargées d'empêcher l'accès aux données et aux sources de données auprès de l'ISF ou de détruire ou de faire détruire, en tout ou en partie, les sources de données. Le Gouvernement flamand fixe les conditions et modalités d'un tel empêchement d'accès ou d'une telle destruction.

## CHAPITRE 7. — Conseiller en sécurité

**Art. 19.** § 1<sup>er</sup>. L'ISF désigne, parmi les membres de son personnel et après avis de la Commission de contrôle flamande, un conseiller en sécurité tel que visé à l'arrêté du Gouvernement flamand du 15 mai 2009 relatif aux conseillers en sécurité.

§ 2. Le conseiller en sécurité de l'ISF exécute ses missions, en vue de la sécurisation des données qui sont traitées ou échangées par l'ISF et en vue de la protection de la vie privée des personnes auxquelles les données ont trait, conformément à l'arrêté du Gouvernement flamand du 15 mai 2009 relatif aux conseillers en sécurité.

Sans préjudice des missions, telles que visées à l'arrêté du Gouvernement flamand du 15 mai 2009 relatif aux conseillers en sécurité, le conseiller en sécurité collabore avec les conseillers en sécurité des autres instances, autorités externes et intégrateurs de services pour arriver à une approche cohérente de la protection des informations. Le conseiller en sécurité de l'ISF veille également à la sensibilisation de la protection des informations auprès des instances en question. Le Gouvernement flamand peut également imposer des missions complémentaires au conseiller en sécurité de l'ISF.

Le respect des exigences de sécurité, telles que fixées à l'article 16 de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard du traitement de données à caractère personnelle, par l'ISF et les utilisateurs de l'ISF sera évalué chaque année par la Commission de contrôle flamande.

## CHAPITRE 8. — Le comité de coordination

**Art. 20.** Un comité de coordination est institué auprès de l'ISF. Il se compose de représentants des instances et des administrations provinciales et locales. Tous les intégrateurs de services flamands font également partie du comité de coordination.

Le comité de coordination assiste l'ISF dans l'exécution de ses missions. A cet effet, le comité de coordination propose des initiatives en vue de favoriser et de consolider les prestations de services électroniques en faveur des instances et autorités externes et propose toutes les mesures utiles susceptibles de contribuer à un traitement sécurisé et confidentiel de données à caractère personnel ou à une simplification administrative pour les instances en question.

Le comité de coordination peut créer en interne des groupes de travail à qui il confie des tâches particulières. Il établit son règlement d'ordre intérieur et le soumet pour approbation au Gouvernement flamand.

**Art. 21.** Le comité de coordination remet à l'ISF des avis concernant :

- 1° l'accès possible à des sources de données ou sources de données authentiques par le biais de l'ISF;
- 2° l'adaptation éventuelle des sources de données de sorte que, dans la mesure du possible, seules des données authentiques soient rendues accessibles;
- 3° l'optimisation, au sein des instances, de la création, de l'utilisation, de l'échange et de la gestion de sources de données et de sources de données authentiques :
- 4° une approche structurée lors de la mise en place d'un système de sources de données authentiques flamandes, y compris la promotion, l'encadrement et la coordination de sources de données authentiques auprès des instances;
- 5° l'utilisation de renvois à la donnée dans la source de données ou la source de données authentique en ce qui concerne des données qui regroupent, partiellement ou dans leur ensemble, une donnée authentique dans une source de données authentique;
- 6° l'établissement de règles pour la source de données ou la source de données authentique concernant les conditions de consultation par ou de communication à une instance demandeuse de données déterminées.

Le comité de coordination délibère sur des initiatives visant à promouvoir et à maintenir la collaboration en matière d'échange électronique de données et des initiatives susceptibles de contribuer à un traitement légitime et confidentiel des données.

Le comité de coordination peut également remettre des avis ou formuler des recommandations concernant l'informatisation et l'échange électronique de données administratives ou des matières apparentées, formuler des propositions pour ou collaborer à l'organisation de cours de formation en matière d'informatique et d'échange électronique de données administratives au profit du personnel des instances et examiner comment l'échange rationnel de données peut être stimulé.

Le comité de coordination délibère, de sa propre initiative ou à la demande du Gouvernement flamand, d'un membre du Gouvernement flamand, de l'ISF ou d'une instance. Le Gouvernement flamand peut déterminer dans quels cas la consultation du comité de coordination est obligatoire.

Les membres du comité de coordination visent à un consensus. A défaut de consensus, le comité de coordination reflète les différents points de vue dans l'avis et la délibération.

**Art. 22.** Le comité de coordination est convoqué au moins une fois l'an à l'initiative du président et chaque fois qu'un des membres du comité de coordination le demande.

Le Gouvernement flamand fixe la composition du comité de coordination, détermine la composition et le fonctionnement du secrétariat chargé du soutien administratif et l'organisation du comité de coordination, décrit, au besoin, ses compétences en détail, fixe les modalités d'application au fonctionnement et désigne le président et les membres.

L'ISF supporte les frais de fonctionnement du comité de coordination et des groupes de travail qui y sont créés.

#### CHAPITRE 9. — Dispositions de modification et finales

**Art. 23.** Dans le décret du 22 décembre 2006 contenant diverses mesures d'accompagnement du budget 2007, modifié par les décrets des 21 décembre 2007, 19 décembre 2008 et 23 décembre 2010, les modifications suivantes sont apportées :

1° le titre du chapitre XXIII est remplacé par ce qui suit : « Chapitre XXIII. DAB Informatie Vlaanderen » (SGS Information Flandres)

2° à l'article 79, § 1<sup>er</sup>, les termes « ICT (DAB ICT) (SGS TIC) » sont remplacés par les termes « Informatie Vlaanderen » (Information Flandres);

3° à l'article 79, § 2, les termes « DAB ICT » (SGS TIC) sont remplacés par les termes « DAB Informatie Vlaanderen » (SGS Information Flandres);

4° à l'article 79, § 2bis, inséré par le décret du 19 décembre 2008, les modifications suivantes sont apportées :

a) les termes « DAB ICT » (SGS TCI) sont remplacés par les termes « DAB Informatie Vlaanderen » (SGS Information Flandres);

b) au deuxième alinéa, une phrase est ajoutée, dont la teneur est la suivante : « Il remplit la fonction d'intégrateur de services conformément au décret portant création et organisation d'un intégrateur de services flamand. »;

5° à l'article 79, § 3, les termes « DAB ICT » (SGS TCI) sont remplacés dans chaque cas par les termes « DAB Informatie Vlaanderen » (SGC Information Flandres);

**Art. 24.** A l'article 2, 15°, du décret du 18 juillet 2008 relatif à l'échange électronique de données administratives, les modifications suivantes sont apportées;

1° les termes « Autorité flamande » sont remplacés par les termes « entités de l'administration flamande ou d'administrations provinciales et locales »;

2° entre le terme « de » et le terme « réglementation », le terme « flamande » et inséré.

**Art. 25.** Dans le même décret, la section II du chapitre II, qui se compose de l'article 5, est supprimée.

**Art. 26.** Dans les deux ans suivant l'entrée en vigueur du présent décret, le Gouvernement flamand fera rapport au Parlement flamand de l'application du présent décret, le cas échéant, moyennant ajoute de recommandations susceptibles de déboucher sur une initiative décrétable ou d'autres mesures en vue d'une exécution appropriée du présent décret. Le rapport est basé sur un rapport d'évaluation de l'ISF en soi, un rapport d'évaluation de la commission de contrôle flamande et un rapport du comité de coordination, visé à l'article 20.

**Art. 27.** Le présent décret entre en vigueur le jour de sa publication au *Moniteur belge*.

Promulguons le présent décret, ordonnons qu'il soit publié au *Moniteur belge*.

Bruxelles, le 13 juillet 2012.

Le ministre-président du Gouvernement flamand,  
K. PEETERS

Le ministre flamand de la Gouvernance publique, de l'Administration intérieure,  
de l'Intégration civique, du Tourisme et de la Périphérie flamande.  
G. BOURGEOIS

—  
Note

(1) *Séance 2011-2012.*

*Documents.* — Projet de décret, 1516 - N° 1. — Rapport, 1516 - N° 2. — Texte adopté en séance plénière, 1516 - N° 3.

*Annales.* — Discussion et adoption. Séance du matinale et nocturne du 4 juillet 2012.