Federale Overheidsdienst
Mobiliteit en Vervoer
Mobiliteit en Verkeersveiligheid

OVEREENKOMST TOT MEDEDELING VAN GEGEVENS
tussen
de FOD Justitie
en
het Directoraat-generaal Wegvervoer en Verkeersveiligheid
van de Federale Overheidsdienst (FOD) Mobiliteit en Vervoer

1. KADER EN VOORWERP VAN DE OVEREENKOMST

De FOD Justitie en de gerechtelijke instanties hadden, in het kader van de werkzaamheden van hun diensten, in het verleden reeds toegang tot het repertorium van de voertuigen zoals bedoeld in artikel 6 van het koninklijk besluit van 20 juli 2001 betreffende de inschrijving van voertuigen[1]. Deze toegang bestond reeds vooraleer artikel 36bis in de WVP[2] werd ingevoegd en dus nog vooraleer de FOD Mobiliteit en Vervoer een modernisering van het informatiesysteem van het repertorium van de voertuigen doorvoerde. Deze modernisering hield in dat voortaan niet langer gebruik zou worden gemaakt van de X25 – verbinding, maar van het TCP/IP-protocol.

Naar aanleiding van deze modernisering waarbij de FOD Mobiliteit en Vervoer aan de FOD Justitie vroeg om hieraan mee te werken in de zin van een aanpassing van de toegangsmodaliteiten, heeft de FOD Justitie een machtigingsaanvraag ingediend bij het Sectoraal Comité voor de Federale Overheid[3] om zich in regel te stellen met artikel 36bis WVP. Het SCFO heeft bij beraadslaging nr. 23/2010 van 21 december 2010 machtiging verleend aan de FOD Justitie om toegang te verkrijgen tot bepaalde gegevens uit het DIV-repertorium.

Deze overeenkomst legt aldus de regels vast voor de mededeling van gegevens uit het DIV-repertorium aan de FOD Justitie en de gerechtelijke instanties. De machtiging van het SCFO staat dan ook de volgende bepalingen toe.

De gevraagde gegevens zullen worden gebruikt in het kader van de volgende doeleinden:
- de uitvoering van de taken van de magistratuur;
- de mededeling van de tenaamgestelde van een voertuig aan buitenlandse gerechtelijke autoriteiten door de Centrale Autoriteit Internationale Samenwerking in Strafzaken;
- de opdrachten van bepaalde ambtenaren van de Veiligheid van de Staat.

---

[1] Hierna "DIV-repertorium".
[2] Artikel 36bis werd in de WVP ingevoegd bij wet van 26 februari 2003 tot wijziging van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens en van de wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de Commissie voor de bescherming van de persoonlijke levenssfeer en tot uitbreiding van haar bevoegdheden.
[3] Hierna "SCFO".

Hiervoor zal toegang worden verleend aan:
1) magistraten en medewerkers binnen de Rechterlijke macht, meer bepaald :
- de staande magistratuur;
- de zittende magistratuur, voor zover de magistraten die de gegevens iot het DIV-repertorium raadplegen dit doen in het kader van een onderzoeksopdracht zoals omschreven in het Wetboek van Strafvordering, het Gerechtelijk Wetboek en/of de bijzondere wetten;
- de medewerkers van magistraten, voor zover zij de gegevens uit het DIV-repertorium enkel raadplegen in het kader van de hen door de wetgeving toegekende opdrachten.
2) de ambtenaren van de FOD Justitie die werkzaam zijn bij de Centrale Autoriteit Internationale Samenwerking in Strafzaken (een entiteit van de FOD Justitie);
3) de applicatiebeheerders en systeembeheerders binnen de Stafdienst ICT (Directie Infrastructuur) van de FOD Justitie;
4) medewerkers van de Veiligheid van de Staat (eveneens een entiteit van de FOD Justitie).

Het SCFO is van oordeel dat de gegevens zolang mogen worden bewaard, totdat deze niet langer nuttig zijn, dat de permanente toegang tot deze gegevens in deze noodzakelijk is en dat de toegang voor onbepaalde duur ook noodzakelijk is.

De nieuwe technologie gebruikt in het kader van de toegang tot de gegevens uit het DIV-repertorium, is gebaseerd op de toepassing van de aanbevelingen die de FOD Mobiliteit en Vervoer voorstelt in het document 'Consultation of titular data_V02d'.

Deze nieuwe technologie berust op het beginsel van uitwisseling van gegevens via Webservices, als basis voor de raadpleging van voertuiggegevens en de daaraan gekoppelde persoonsgegevens die zich bevinden in het DIV-repertorium.

De invoering van deze nieuwe technologie gebeurt in een server-to-server-structuur van het type (B2B). Als veiligheidsbeginsel voor dit soort uitwisseling wordt gebruik gemaakt van een filtering op het niveau van de IP-adressen (Internet Protocol) en de activering van wederzijdse certificaten die de echtheid van beide partijen waarborgt. Door gebruik te maken van het HyperText Transfer Protocol Secure (HTTPS)-protocol kan de verbinding van end-to-end beveiligd worden.

Om te voldoen aan de eisen van de FOD Mobiliteit en Vervoer bij het gebruik van Webservices als uitwisselingsmiddel ter vervanging van de thans gebruikte X25, heeft de dienst IT van de FOD Justitie mechanismen ontwikkeld of aangepast die het volgende garanderen:
- individuele identificatie van de gebruiker van de toepassing die toegang biedt tot het DIV-repertorium;
- authenticatieproces van de gebruiker om steeds de link tussen de gebruiker van de dienst en de natuurlijke persoon te garanderen;
- beperking van de toegang tot informatie naargelang de rol van de gebruiker;
- traceerbaarheid van het gebruik van de dienst waardoor te allen tijde een link kan worden gelegd tussen de gebruiker en zijn verzoek (de WIE, WAT, WANNEER en HOE beginselen).

2. VERANTWOORDELIJKEN VOOR DE VERWERKING

In de zin van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer zijn de verantwoordelijken voor de verwerking:

a) De Directie Inschrijvingen Homologaties Voertuigen (DIV), die deel uitmaakt van het Directoraat-generaal Wegvervoer en Verkeersveiligheid van de Federale Overheidsdienst Mobiliteit en Vervoer (ondernemingsnummer 0308357852), met zetel in het City Atrium, Vooruitgangstraat 56 te 1210 Brussel (Sint-Joost-ten-Node) en vertegenwoordigd door de heer Marnix SCHEERLINCK, Adviseur-generaal Directie Inschrijvingen en Homologaties Voertuigen.
De DIV handelt als verantwoordelijke voor de verwerking, met name als openbaar bestuur dat gegevens van zijn DIV-repertorium verzamelt en meedeelt.
b) De FOD Justitie, gelegen te 1000 Brussel, Waterloolaan 115, vertegenwoordigd door de heer J.P. Janssens, Voorzitter van het directiecomité.
De FOD Justitie handelt als verantwoordelijke voor de verwerking, met name als instelling die gegevens van het DIV-repertorium ontvangt en verwerkt in de zin van deze overeenkomst.

De DIV en de FOD Justitie handelen derhalve als verantwoordelijken voor de verwerking, als instellingen die het doel en de middelen voor de verwerking van persoonsgegevens bepalen (artikel 1, § 4, van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer).

3. VERSTREKKER EN ONTVANGER VAN DE GEGEVENS

De verstrekker van de gegevens is de DIV, beter geïdentificeerd in punt 2.a hierboven. De ontvanger van de gegevens is de FOD Justitie, beter geïdentificeerd in punt 2.b hierboven.

4. DOELSTELLING(EN) GOEDGEKEURD DOOR HET SECTORAAL COMITÉ VOOR DE FEDERALE OVERHEID

Onder voorbehoud van de eventueel in de toelating van het SCFO vermelde voorwaarden, mag de FOD Justitie de gegevens van het DIV-repertorium uitsluitend voor de onderstaande, door het SCFO toegestane, doeleinden gebruiken:

a) de strafrechtelijke opsporing en vervolging van misdaden, wanbedrijven en overtredingen ;
b) de politie over het wegverkeer en de verkeersveiligheid, de veiligheid van de motorvoertuigen en aanhangwagens inbegrepen;
c) het toezicht op de dekking van de burgerrechtelijke aansprakelijkheid waartoe de motorvoertuigen en aanhangwagens aanleiding kunnen geven;
d) de kennisgeving aan de bij een verkeersongeval betrokken partijen, van de identiteit van de verzekeringsmaatschappijen die de burgerrechtelijke aansprakelijkheid dekken als gevolg van het gebruik van elk der bij dat ongeval betrokken voertuigen;

Ieder ander doeleinde dat niet formeel door het SCFO werd goedgekeurd, wordt niet als legitiem gebruiksdoel beschouwd.

5. MEEGEDEELDE GEGEVENS EN UITVOERINGSMODALITEITEN

Zie in bijlage de machtiging nr. 23/2010 van 21 december 2010, afkomstig van het SCFO, opgericht binnen de Commissie voor de Bescherming van de Persoonlijke Levenssfeer, ~~alsook het document 'Consultation of titular data_V02d'.~~

6. VERWERKING

a) Indien de verwerking wordt toevertrouwd aan een verwerker, bijvoorbeeld een ICT-dienst, moet de verantwoordelijke voor de verwerking, en in voorkomend geval zijn vertegenwoordiger in België:
   1° een verwerker kiezen die voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerking;
   2° toezien op de naleving van die maatregelen, met name door ze vast te leggen in contractuele bepalingen;
   3° de aansprakelijkheid van de verwerker ten aanzien van de verantwoordelijke voor de verwerking vaststellen in de overeenkomst;
   4° met de verwerker overeenkomen dat de verwerker slechts handelt in opdracht van de verantwoordelijke voor de verwerking en dat de verwerker is gebonden door dezelfde verplichtingen als die waartoe de verantwoordelijke in toepassing van de bepalingen van punt c hieronder is gehouden;
   5° in een geschrift of op een elektronische drager de elementen van de overeenkomst met betrekking tot de bescherming van de gegevens en de eisen met betrekking tot de maatregelen bedoeld in de bepalingen van punt c hieronder vaststellen.

b) Indien de ontvanger een verwerker kiest, moet daarvoor dus een contract worden opgesteld en moet een kopie daarvan worden overgezonden aan de verstrekker (de DIV); dit contract maakt een wezenlijk deel uit van deze overeenkomst. De door de ontvanger gekozen verwerker moet de bepalingen van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer op alle punten in acht nemen.

c) Eenieder die handelt onder het gezag van de verantwoordelijke voor de verwerking of van de verwerker alsmede de verwerker zelf, die toegang heeft tot persoonsgegevens, mag deze slechts in opdracht van de verantwoordelijke voor de verwerking verwerken, behoudens op grond van een verplichting door of krachtens een wet, een decreet of een ordonnantie.

d) Bij gebrek aan instructies vanwege de verantwoordelijke voor de verwerking of aan een verplichting door of krachtens een wet, een decreet of een ordonnantie, moet de verwerker afzien van de verwerking van persoonsgegevens en mag hij geen enkel initiatief terzake nemen.

e) Indien de ontvanger ingrijpende wijzigingen aanbrengt in de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerking, zoals andere informatica of een andere verwerker bijvoorbeeld, moet dat worden gemeld aan de verstrekker (de DIV).

7. NORMATIEVE GRONDSLAGEN

a) <u>Voor de DIV:</u>
   - Wet van 16 maart 1968 betreffende de Politie over het Wegverkeer
   - artikel 6 van het koninklijk besluit van 20 juli 2001 betreffende de inschrijving

van voertuigen alsook het krachtens dit koninklijk besluit aangelegde repertorium.

b) Voor de FOD Justitie:
   - artikel 6 van het koninklijk besluit van 20 juli 2001 betreffende de inschrijving van voertuigen alsook het krachtens dit koninklijk besluit aangelegde repertorium.

8. VOORWAARDEN VAN DE OVEREENKOMST

a) Met de ondertekening van deze overeenkomst verbindt elk van de partijen zich tot inachtneming van de voorwaarden en modaliteiten in de overeenkomst en haar eventuele bijlagen, met name de bewaarperiode voor de uit het DIV-repertorium ontvangen persoonsgegevens, die niet langer mag duren dan noodzakelijk voor de verwezenlijking van de doelstellingen waarvoor ze worden verkregen of verder worden verwerkt;
b) Een aanvraag die het kader en het voorwerp van een verwerking van persoonsgegevens bepaalt, moet vooraf worden gericht aan het SCFO. Voordat dit laatste zijn machtiging verleent, gaat het na of de beoogde mededeling van gegevens conform de wettelijke en reglementaire bepalingen is. Alleen op die voorwaarde kan de DIV een overeenkomst voor de mededeling van gegevens sluiten met de verzoeker. De machtiging van het SCFO en de eventuele voorwaarden maken een wezenlijk deel van de overeenkomst uit, in de vorm van een schriftelijke bijlage. De DIV behoudt zich het recht voor rechtstreeks bij dit Sectoraal Comité bevestiging van deze machtiging te vragen vóór de inwerkingtreding van de overeenkomst.
   Deze bepaling is een *conditio sine qua non* voor het sluiten van een overeenkomst tot mededeling van persoonsgegevens tussen de verstrekker, zijnde de DIV, en een potentiële ontvanger.

9. WIJZIGINGEN VAN DE OVEREENKOMST

Wijzigingen in de tekst en het principe van deze overeenkomst moeten verplicht deel uitmaken van een nieuwe schriftelijke, door beide partijen goedgekeurde en ondertekende overeenkomst.

10.CONTACTPUNTEN

a) Voor de FOD Justitie: ICT.Security@just.fgov.be
b) Voor de DIV: help.div@mobilit.fgov.be

11. GEBRUIK EN BEVEILIGING VAN DE GEGEVENS

a) De ontvanger is verplicht om alle nodige voorzorgsmaatregelen te nemen voor de veiligheid van de ontvangen gegevens en is daar ingevolge de bepalingen in deze overeenkomst verantwoordelijk voor. De ontvanger kan zich laten bijstaan door een informatieveiligheidsadviseur, verantwoordelijk voor de uitvoering van het veiligheidsbeleid van de FOD Justitie, hetzij intern of bij een gespecialiseerde derde, met name aangeduid daar deze persoon normaal het eerste contact zal zijn bij problemen. Deze veiligheidadviseur kan ook worden gekozen op sectorniveau voor meerdere ontvangers.

b) Met de ondertekening van deze overeenkomst is de ontvanger zeker dat de netwerken waarmee de bij de verwerking van persoonsgegevens betrokken voorzieningen in verbinding staan, de vertrouwelijkheid en de integriteit van die persoonsgegevens waarborgen.
c) Elk gebruik van de ontvangen gegevens anders dan in deze overeenkomst bepaald is strikt verboden en heeft zonder meer de nietigverklaring van deze overeenkomst tot gevolg, overeenkomstig punt 14 (nietigheidsclausule – sanctie).
d) De Directie Inschrijvingen en Homologaties Voertuigen (DIV), die deel uitmaakt van het Directoraat-generaal Wegvervoer en Verkeersveiligheid van de Federale Overheidsdienst Mobiliteit en Vervoer, behoudt zich het recht tot audits en steekproeven voor, zo nodig bij de betrokkenen bij de verwerking van persoonsgegevens maar ook bij de ontvanger, om te controleren of deze laatste zijn verbintenissen ten aanzien van deze overeenkomst nakomt.
e) De FOD Justitie, als ontvanger van de gegevens, verbindt zich ertoe te allen tijde inzagerecht te verlenen aan de DIV, de CBPL en het SCFO, alsook aan hun vertegenwoordigers vernoemd op alle als voor deze diensten relevant beschouwde documenten, en op al hun vragen te antwoorden.
In voorkomend geval kunnen deze personen een bezoek of een consultatie ter plaatse, al dan niet van tevoren aangekondigd, verrichten om te controleren of de ontvanger of zijn eventuele verwerker de voorwaarden van deze overeenkomst nakomt.
f) De DIV en de FOD Justitie, als verantwoordelijken voor de verwerking, en hun eventuele verwerkers treffen de nodige technische en organisatorische maatregelen om de persoonsgegevens te beschermen tegen toevallige of ongeoorloofde vernietiging, tegen toevallig verlies, alsook tegen de wijziging van of de toegang tot, en iedere andere niet toegelaten verwerking van persoonsgegevens.
Het beveiligingsniveau moet in verhouding staan tot de stand van de techniek terzake, de bijbehorende kosten, de aard van de gegevens en de potentiële risico's.
g) De ontvanger of zijn eventuele verwerker zijn verplicht om een informatieveiligheidsplan op te stellen en een inventaris te maken van alle ontvangen vragen of klachten over de veiligheid van de persoonsgegevens; eventuele incidenten moeten eveneens worden geïnventariseerd.
Ernstige of herhaalde incidenten met betrekking tot de veiligheid van de persoonsgegevens (schending) bij de ontvanger of zijn eventuele verwerker moeten worden meegedeeld aan de verstrekker (de DIV). Deze laatste oordeelt of de bevoegde gerechtelijke overheden moeten worden verwittigd, rekening houdend met de strafbepalingen in de artikelen 37 tot 43 WVP. In de kennisgeving aan de gerechtelijke overheden door de gegevensverstrekker worden de gevolgen van de schending beschreven, alsook de voorgestelde of getroffen maatregelen om ze te verhelpen.

12. DUUR EN OPZEGGING VAN DE OVEREENKOMST

a) Deze overeenkomst wordt gesloten voor onbepaalde duur en gaat in op de datum van de ondertekening door beide partijen.
b) Ze kan worden opgezegd door een van de partijen met een opzegtermijn van 3 maanden, behoudens uitdrukkelijke bepalingen in punt 13 van deze overeenkomst (nietigheidsclausule – sanctie).

13. NIETIGHEIDSCLAUSULE – SANCTIE

Indien de bepalingen van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer of de bepalingen van deze overeenkomst klaarblijkelijk niet in acht worden genomen, behoudt de DIV, als verstrekker, zich het recht voor de mededeling van gegevens aan de ontvanger te onderbreken, onmiddellijk en na haar controles overeenkomstig punt 11.e en punt 11.f van deze overeenkomst, en geeft ze hem per aangetekende post of per e-mail met ontvangstbevestiging kennis van de redenen ervoor.
Op grond van deze kennisgeving wordt de overeenkomst tussen de FOD Justitie en de DIV van nul en generlei waarde.

De hoven en rechtbanken van Brussel zijn bevoegd voor alle geschillen die voortvloeien uit deze overeenkomst en die niet krachtens deze overeenkomst kunnen worden opgelost.

14. BIJLAGEN

Bijlagen kunnen, indien nodig in detail, de draagwijdte van de samenwerking beschrijven, alsook de eventuele duur van het project, de voorwaarden die moeten worden vervuld en de middelen die moeten worden aangewend door elk van de partijen.

Als bijlagen gaan:

a) Machtiging van het Sectoraal Comité voor de Federale Overheid in verband met deze overeenkomst (bijlage 1).
~~b) Document 'Consultation of titular data_V02d'versie op datum van opmaak van deze overeenkomst (bijlage 2).~~

15. BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER

De verwerking van de aldus verzamelde gegevens gebeurt overeenkomstig de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens en haar toepassingsbesluiten.

De FOD Justitie verbindt zich ertoe de van de DIV ontvangen gegevens louter te gebruiken voor het(de) doeleinde(n) en onder de voorwaarde(n) die in de machtiging nr. 23/2010 van het SCFO zijn beschreven.

16.TRANSPARANTIE

a) De overeenkomstsluitende partijen gaan ermee akkoord dat deze overeenkomst integraal wordt overgenomen op de website van de FOD Mobiliteit en Vervoer: www.mobilit.belgium.be.
b) Papieren exemplaren van deze overeenkomst zijn eveneens beschikbaar op eenvoudige schriftelijke aanvraag bij de DIV of de FOD Justitie, op het in punt 2.a en punt 2.b van deze overeenkomst vermelde postadres of op de e-mailadressen "help.DIV@mobilit.fgov.be" en "ICT.Security@just.fgov.be".

17.VERSCHILLEN IN DE INTERPRETATIE VAN DEZE OVEREENKOMST

De overeenkomstsluitende partijen verbinden zich ertoe om een oplossing te vinden voor de verschillen die zich voordoen bij de interpretatie van deze overeenkomst, haar bijlagen en haar aanhangsels. In geval van een conflict naar aanleiding van een meningsverschil over de interpretatie van deze overeenkomst, zal steeds de beslissing van het SCFO hierover worden gevolgd.

Opgemaakt te Brussel, op 16.05.13 in twee exemplaren, waarbij elke partij erkent een exemplaar te hebben ontvangen.

Voor de FOD Justitie,

J.P. Janssens
Voorzitter Directiecomité

Voor de DIV,

Marnix SCHEERLINCK
Adviseur-generaal Directie Inschrijvingen en Homologaties Voertuigen

Sectoraal comité voor de Federale Overheid

Beraadslaging FO nr 23/2010 van 21 december 2010

Betreft: Machtigingsaanvraag voor de verwerking van gegevens van de DIV door de FOD Justitie en de gerechtelijke instanties (AF/MA/2010/123)

Het Sectoraal comité voor de Federale Overheid;

Gelet op de wet van 8 december 1992 *tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens* (hierna WVP), inzonderheid de artikelen 31*bis* en 36*bis*;

Gelet op het koninklijk besluit van 17 december 2003 *tot vaststelling van de nadere regels met betrekking tot de samenstelling en de werking van bepaalde sectorale comités opgericht binnen de Commissie voor de bescherming van de persoonlijke levenssfeer*, inzonderheid artikel 18;

Gelet op de aanvraag van Dhr. A. Bourlet, Voorzitter van het Directiecomité van de Federale Overheidsdienst Justitie ontvangen op 03/11/2010;

Gelet op de aanvraag van het technisch en juridisch advies gericht aan de Federale Overheidsdienst Fedict op 02/12/2010;

Gelet op het technisch en juridisch advies ontvangen op 16/12/2010;

Gelet op het verslag van de Voorzitter;

Beslist op 21 december 2010, na beraadslaging, als volgt:

I. ONDERWERP EN CONTEXT VAN DE AANVRAAG

1. In zijn machtigingsaanvraag dd. 3 november 2010 verzoekt de FOD Justitie het Comité om toegang te verkrijgen tot het repertorium van de voertuigen van de Dienst Inschrijving Voertuigen van de Federale Overheidsdienst Mobiliteit en Vervoer (hierna "de DIV"). Deze aanvraag werd op 30 november 2010 en 1 december 2010 aangevuld met bijkomende informatie.

2. De gevraagde gegevens zullen door drie verschillende instanties worden gebruikt:
   - de Rechterlijke Macht;
   - de Centrale Autoriteit Internationale Samenwerking in Strafzaken (een entiteit van de FOD Justitie);
   - de Veiligheid van de Staat (eveneens een entiteit van de FOD Justitie).

3. Momenteel beschikken voornoemde instanties reeds over een toegang tot de gevraagde informatie. Naar aanleiding van de invoering van een nieuwe technologie (server-to-server-structuur) om deze toegang in de toekomst verder te operationaliseren, hebben de FOD Justitie en de DIV beslist om ook een aanvraag in te dienen bij het Comité ten einde zich in regel te stellen met artikel 36*bis* WVP.

II. ONDERZOEK VAN DE AANVRAAG

A. BEVOEGDHEID VAN HET COMITE

4. Krachtens artikel 36*bis* WVP, *"vereist elke elektronische mededeling van persoonsgegevens door een federale overheidsdienst of door een openbare instelling met rechtspersoonlijkheid die onder de federale overheid ressorteert een principiële machtiging* (van het bevoegd sectoraal comité)".

5. Het is de taak van dit Comité om na te gaan "*of deze mededeling enerzijds nodig is voor de implementatie van de opdrachten die toevertrouwd worden door of krachtens de wet aan de vragende federale overheid en anderzijds of deze mededeling in zijn diverse aspecten compatibel is met al de geldige normen inzake de bescherming van de persoonlijke levenssfeer wat de verwerking van de persoonsgegevens betreft.*" (Parl. Doc 50, 2001-2002, nr. 1940/004).

6. De DIV, dat deel uitmaakt van de FOD Mobiliteit en Vervoer, zal gegevens elektronisch doorsturen naar de FOD Justitie. In zoverre de uitgewisselde gegevens persoonsgegevens betreffen[1], is het Comité bevoegd om zich over deze elektronische mededeling uit te spreken.

B. TEN GRONDE

1. FINALITEITSBEGINSEL

7. Artikel 4, § 1, 2°, WVP laat de verwerking van persoonsgegevens slechts toe voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en de gegevens mogen bovendien niet verder worden verwerkt op een wijze die onverenigbaar is met die doeleinden. In de hiernavolgende paragrafen onderzoekt het Comité of deze principes in onderhavig geval gerespecteerd worden.

8. Het Comité leidt uit de aanvraag af dat er met de gevraagde toegang drie verschillende finaliteiten beoogd worden:

- voor de uitvoering van de taken van de magistratuur (hierna "eerste doeleinde")
- voor de mededeling van de tenaamgestelde van een voertuig aan buitenlandse gerechtelijke autoriteiten door de Centrale Autoriteit Internationale Samenwerking in Strafzaken (hierna "tweede doeleinde");
- voor de opdrachten van bepaalde ambtenaren van de Veiligheid van de Staat (hierna "derde doeleinde").

9. Voor wat het eerste doeleinde betreft wordt in de aanvraag gewezen op de ruime bevoegdheden van de magistratuur en wordt een algemene beschrijving gegeven van de finaliteiten die met de gevraagde toegang worden nagestreefd:

> *"De rechterlijke macht heeft met betrekking tot de geschillenbeslechting een bevoegdheid die alleen maar beperkt wordt door het grondwettelijke voorschrift dat de Wetgever de geschillen over de door hem bepaalde politieke rechten (lees vooral de bestuurszaken) aan de Macht mag onttrekken. Dat betekent dat, behoudens die uitzonderingsgevallen, alle mogelijke geschillen over alle mogelijke onderwerpen ter beslechting voor de hoven en rechtbanken mogen worden gebracht.[2] (...) Uit het bovenstaande volgt dat het niet mogelijk is de geschillen waarvan de Rechterlijke Macht kennis neemt nauwkeurig op te sommen of te*

---

[1] Er worden ook gegevens omtrent rechtspersonen opgevraagd. Dit zijn geen persoonsgegevens in de zin van artikel 1, § 1, WVP (cf. infra randnummers 23-24).

[2] Zie ook de artikelen 144 en 145 van de Grondwet.

omschrijven. Zulke opsomming of omschrijving zou grote hiaten vertonen zowel op het moment dat zij wordt uitgevoerd als diachronisch want zij zou snel niet meer adequaat zijn wegens de voortdurende evolutie van de samenleving. (...)
Wanneer de Rechterlijke Macht voor de beslechting van eender welk geschil waarvoor zij bevoegd is, gegevens nodig heeft die in verband staan met een voertuig moet zij die gegevens kunnen kennen op gevaar anders haar grondwettelijke en wettelijke opdracht niet naar behoren te kunnen uitvoeren. Dat zou hetzelfde gevolg hebben als rechtsweigering wegens ontstentenis van beslechting of wegens foute beslechting. (...)
Het doeleinde van het gebruik van de gegevens van het repertorium is om een zo exact mogelijke informatie te verkrijgen ten behoeve van de geschillenbeslechting waarvoor de Rechterlijke Macht bevoegd is, ten einde de kwaliteit van die geschillenbeslechting te garanderen en zo de eerbiediging van de rechten van alle betrokkenen te waarborgen."

10. In de aanvraag wordt hier aan toegevoegd dat de raadpleging meestal zal worden verricht door de parketten (de magistraten van het openbaar ministerie) en de onderzoekrechters en de door hen aangewezen medewerkers (de parketsecretarissen, de griffiers en leden van het parket –en griffiepersoneel). Daarnaast zal het aldus de FOD Justitie de rechtsgang bevorderen als de magistraten van de vonnisgerechten en de magistraten van de burgerlijke gerechten en de door hen aangewezen medewerkers (de grifflers en het griffiepersoneel) het repertorium mogen raadplegen om de exactheid van de gegevens te controleren die de gedingpartijen of andere bij het proces betrokken personen aanbrengen.

11. Het Comité onderschrijft, aangaande het eerste doeleinde, het standpunt van de FOD Justitie, met name dat het niet mogelijk is om een gedetailleerde en exhaustieve opsomming te geven van de gevallen waarin de rechterlijke macht toegang wenst tot de gevraagde gegevens. Het beslist dat de omschrijving die wordt geciteerd in randnummer 9 volstaat opdat sprake zou zijn van welbepaalde en uitdrukkelijk omschreven doeleinden in de zin van artikel 4, § 1, 2°, WVP. Het stelt zich wel ernstige vragen bij het voorstel om toegang te verlenen tot alle leden van de zittende magistratuur alsook tot alle medewerkers die door magistraten zijn aangewezen. Het Comité ziet geen redelijke verantwoording voor een dergelijke ruime toegang en het beslist om deze te beperken tot:

- de staande magistratuur;
- de zittende magistratuur, voor zover de magistraten die de DIV-gegevens raadplegen dit doen in het kader van een onderzoeksopdracht zoals omschreven in het Wetboek van Strafvordering, het Gerechtelijk Wetboek en/of de bijzondere wetten;
- de medewerkers van magistraten, voor zover zij de DIV-gegevens enkel raadplegen in het kader van de hen door de wetgeving toegekende opdrachten.

12. Voor wat het tweede doeleinde betreft wordt verduidelijkt dat de gegevens aan buitenlandse gerechtelijke autoriteiten zullen doorgegeven worden in gevallen waarin er in hun land verkeersovertredingen of andere misdrijven worden gepleegd met voertuigen die bij de DIV zijn ingeschreven. Het Comité is van oordeel dat dit eveneens een welbepaald en uitdrukkelijk omschreven doeleinde betreft.

13. Ook wat het derde doeleinde betreft komt het Comité tot dezelfde conclusie. De bevoegde medewerkers zullen deze toegang immers gebruiken in het kader van de verwezenlijking van de opdrachten van de Staatsveiligheid, met name:

> *"De Veiligheid van de Staat heeft als opdracht :*
> *1° het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op elke activiteit die de inwendige veiligheid van de Staat en het voortbestaan van de democratische en grondwettelijke orde, de uitwendige veiligheid van de Staat en de internationale betrekkingen, het wetenschappelijk of economisch potentieel, zoals gedefinieerd door het Ministerieel Comité, of elk ander fundamenteel belang van het land, zoals gedefinieerd door de Koning op voorstel van het Ministerieel Comité, bedreigt of zou kunnen bedreigen;*
> *2° het uitvoeren van de veiligheidsonderzoeken die haar overeenkomstig de richtlijnen van het Ministerieel Comité worden toevertrouwd;*
> *3° het uitvoeren van de opdrachten tot bescherming van personen die haar worden toevertrouwd door de Minister van Binnenlandse Zaken;*
> *4° het uitvoeren van alle andere opdrachten die haar door of krachtens de wet worden toevertrouwd."*[3]

14. Het Comité vestigt er de aandacht op dat de gevraagde gegevens enkel mogen gebruikt worden voor de drie doeleinden die in de machtigingsaanvraag zijn opgesomd (cf. supra randnummer 8).

15. Aangaande de vereiste van verenigbaarheid met het oorspronkelijk doeleinde, wijst het Comité erop dat de geplande verwerkingen, met name de doorgifte van bepaalde gegevens door de DIV aan de drie hoger genoemde instanties, bestaan uit latere verwerkingen van gegevens die oorspronkelijk voor andere doeleinden werden verwerkt. De rechtmatigheid van deze latere verwerkingen is aldus afhankelijk van hun verenigbaarheid met de oorspronkelijke verwerking. Dit onderzoek naar de verenigbaarheid wordt gedaan in functie van de redelijke verwachtingen van de betrokkene en van de toepasselijke wettelijke en reglementaire bepalingen.

---

[3] Artikel 7 van de wet van 30 november 1998 *houdende regeling van de inlichtingen- en veiligheidsdienst.*

16. In dit verband stelt het Comité aangaande het eerste doeleinde vast dat:

- de artikelen 144 en 145 van de Grondwet het volgende stipuleren:
  "Art. 144. Geschillen over burgerlijke rechten[4] *behoren bij uitsluiting tot de bevoegdheid van de rechtbanken.*
  Art. 145. Geschillen over politieke rechten behoren tot de bevoegdheid van de rechtbanken, behoudens de bij de wet gestelde uitzonderingen."

- artikel 6 van het koninklijk besluit van 20 juli 2001 *betreffende de inschrijving van voertuigen* (hierna KB van 20 juli 2001) het volgende bepaalt:
  "Art. 6. § 2. De doeleinden waarvoor de persoonsgegevens van het repertorium mogen worden verwerkt, zijn :
  1° de strafrechtelijke opsporing en vervolging van misdaden, wanbedrijven en overtredingen; (...)
  10° het bewarend beslag en de tenuitvoerlegging op motorvoertuigen en aanhangwagens;
  11° de politie over het wegverkeer en de verkeersveiligheid, de veiligheid van de motorvoertuigen en aanhangwagens inbegrepen; (...)
  15° het toezicht op de dekking van de burgerrechtelijke aansprakelijkheid waartoe de motorvoertuigen en aanhangwagens aanleiding kunnen geven;
  16° de kennisgeving aan de bij een verkeersongeval betrokken partijen, van de identiteit van de verzekeringsmaatschappijen die de burgerrechtelijke aansprakelijkheid dekken als gevolg van het gebruik van elk de bij dat ongeval betrokken voertuigen; (...)"[5]

17. Het Comité concludeert aldus dat er, voor wat het eerste doeleinde betreft, een voldoende duidelijk regelgevend kader bestaat om een verenigbare latere verwerking te waarborgen.

18. Aangaande het tweede doeleinde constateert het Comité dat:

- artikel 3, 1ste lid, van het Europees Verdrag van 20 april 1959 *aangaande wederzijdse rechtshulp in strafzaken* het volgende stipuleert:
  "De aangezochte Partij geeft volgens de procedure voorzien in haar eigen wetgeving gevolg aan de ambtelijke opdrachten aangaande een strafzaak die tot haar worden gericht door de rechterlijke autoriteiten van de verzoekende Partij en die tot doel hebben het verrichten van

---

[4] In de grondwettelijke betekenis van het woord betekent "geschillen over burgerlijke rechten" alle geschillen die niet de politieke rechten betreffen. Bij de geschillen over deze burgerlijke rechten behoren ook de strafzaken.

[5] Het Comité stelt overigens ook vast dat de wet van 19 mei 2010 *houdende oprichting van de Kruispuntbank van de voertuigen* (B.S. 28 juni 2010) in gelijkaardige regels voorziet (cf. artikel 5, 7°, 16°, 17°, 21°, 22 °, van deze wet). Deze wet is evenwel nog niet in werking getreden (cf. artikel 40).

daden van onderzoek of de toezending van stukken van overtuiging, van dossiers of van documenten."

- artikel 53 van de Overeenkomst van 19 juni 1990 *ter uitvoering van het tussen de Regeringen van de Staten van de Benelux Economische Unie, De Bondsrepubliek Duitsland, en de Franse Republiek op 14 juni 1985 te Schengen gesloten akkoord betreffende de geleidelijke afschaffing van de controles aan de gemeenschappelijke grenzen* het volgende vermeldt:
  "1. Verzoeken om rechtshulp kunnen rechtstreeks tussen de rechterlijke autoriteiten worden gedaan en beantwoord.
  2. Het bepaalde in lid 1 sluit niet uit dat verzoeken tussen Ministeries van Justitie dan wel door tussenkomst van de nationale centrale bureaus van de Internationale Politie-organisatie (Interpol) worden gedaan en beantwoord."

- artikel 6 van het KB van 20 juli 2001 het volgende bepaalt:
  "Art. 6. § 2. De doeleinden waarvoor de persoonsgegevens van het repertorium mogen worden verwerkt, zijn :
  1° de strafrechtelijke opsporing en vervolging van misdaden, wanbedrijven en overtredingen; (...)
  10° het bewarend beslag en de tenuitvoerlegging op motorvoertuigen en aanhangwagens;
  11° de politie over het wegverkeer en de verkeersveiligheid, de veiligheid van de motorvoertuigen en aanhangwagens inbegrepen; (...)[6]

19. Het Comité constateert aldus dat er, voor wat het tweede doeleinde betreft, eveneens een voldoende duidelijk regelgevend kader bestaat om een verenigbare latere verwerking te waarborgen.

20. Voor wat het derde doeleinde betreft, stelt het Comité vast dat:

- artikel 14 van de wet van 30 november 1998 *houdende regeling van de inlichtingen –en veiligheidsdiensten* het volgende bepaalt:
  "(...) Met inachtneming van de geldende wetgeving kunnen de inlichtingen- en veiligheidsdiensten, overeenkomstig de door de Koning vastgelegde algemene nadere regels, toegang krijgen tot de gegevensbanken van de openbare sector die nuttig zijn voor de uitoefening van hun opdrachten."

---

[6] Het Comité stelt overigens ook vast dat de wet van 19 mei 2010 *houdende oprichting van de Kruispuntbank van de voertuigen* (B.S. 28 juni 2010) in gelijkaardige regels voorziet (cf. artikel 5, 7°, 16°, 17°, van deze wet). Deze wet is evenwel nog niet in werking getreden (cf. artikel 40).

- de artikelen 3 en 4 van het koninklijk besluit van 12 oktober 2010 *houdende uitvoering van diverse bepalingen van de wet van 30 november 1998 houdende regeling van de inlichtingen -en veiligheidsdiensten*[7] het volgende stipuleren:

  "Art. 3. § 1. Voor de toepassing van artikel 14, vierde lid, van de wet van 30 november 1998, wanneer de inlichtingen- en veiligheidsdiensten kunnen beschikken over rechtstreekse toegang tot een gegevensbank van de openbare sector die persoonsgegevens bevat, houdt het betrokken diensthoofd permanent de nominatieve lijst van de personen die gemachtigd zijn om toegang te hebben tot de gegevensbank ter beschikking van de Commissie voor de bescherming van de persoonlijke levenssfeer, met vermelding van hun titel en hun functie.

  Bij iedere aanvraag tot raadpleging van een gegevensbank wordt de identiteit van de aanvrager opgetekend in een controlesysteem binnen de betrokken inlichtingen- en veiligheidsdienst. Deze informatie wordt tien jaar bewaard. (...)

  Art. 4. § 1. Door de bevoegde minister wordt op voordracht van het betrokken diensthoofd een raadgever informatieveiligheid en bescherming van de persoonlijke levenssfeer, die onder meer de functie vervult van aangestelde voor de gegevensbescherming, zoals bedoeld in artikel 17bis van de wet van 8 december 1992, aangesteld binnen iedere inlichtingen- en veiligheidsdienst.

  Hij valt onder het rechtstreekse gezag van het diensthoofd aan wie hij uitsluitend rekenschap aflegt en verslag uitbrengt. Hij is op onafhankelijke wijze belast met :

  - het waarborgen van de naleving van de wet bij iedere vraag om gegevens;

  - het nemen van alle nuttige maatregelen teneinde de veiligheid van de geregistreerde informatie te verzekeren;

  - het verstrekken van passende adviezen aan het diensthoofd;

  - het uitvoeren van andere opdrachten die hem door het diensthoofd toevertrouwd zijn.

  De raadgever informatieveiligheid en bescherming van de persoonlijke levenssfeer bedoeld in het eerste lid kan zich door één of meer adjuncten laten bijstaan.

  § 2. Wat de Veiligheid van de Staat betreft, wordt de functie van raadgever informatieveiligheid en bescherming van de persoonlijke levenssfeer, die onder meer de functie vervult van aangestelde voor de gegevensbescherming bedoeld in § 1, uitgeoefend door de raadsman voor de veiligheid van de gegevens aangesteld door de Minister van Justitie overeenkomstig artikel 6 van het koninklijk besluit van 28 februari 2002 betreffende de mededeling van informatie door de gemeenten aan de Veiligheid van de Staat door toedoen van het Rijksregister van de natuurlijke personen."

---

[7] Zie ook het gunstig advies van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer (nr. 24/2010 van 30 juni 2010) toen dit KB nog in voorbereiding was.

21. Het Comité constateert aldus dat er, voor wat het laatste doeleinde betreft, eveneens een voldoende duidelijk regelgevend kader bestaat om een verenigbare latere verwerking te waarborgen.

2. PROPORTIONALITEITSBEGINSEL

2.1. Aard van de gegevens

22. Artikel 4, § 1, 3°, WVP stelt dat persoonsgegevens toereikend, terzake dienend en niet overmatig dienen te zijn, uitgaande van de doeleinden waarvoor zij worden verkregen of waarvoor zij verder worden verwerkt.

23. De FOD Justitie stelt in zijn aanvraag dat de magistratuur, de Centrale Autoriteit Internationale Samenwerking in Strafzaken en de Veiligheid van de Staat, om de finaliteiten zoals omschreven in randnummer 8 te verwezenlijken, de volgende gegevens moeten kunnen raadplegen:

- naam, voornaam, geboortedatum, Rijksregisternummer en adres[8] [9] van de persoon onder wiens naam het voertuig is ingeschreven;
- het adres van het tijdelijke verblijfplaats van de personen bedoeld in artikel 5, § 1, 1° en 2° van het KB van 20 juli 2001;
- naam, rechtsvorm en BTW-nummer van de rechtspersoon op wiens naam het voertuig is ingeschreven;
- het inschrijvingsnummer (het nummer van de kentekenplaat) van het voertuig;
- de datum van eerste inschrijving van het voertuig (in België of in het buitenland);
- het merk of, als het merk niet bekend is, de naam van de bouwer van het voertuig;
- het type en in voorkomend geval de variant en de versie betreffende dit type van het voertuig;
- de handelsnaam van het voertuig;
- het identificatienummer (chassisnummer) van het voertuig;
- de geldigheidsduur van de inschrijving (enkel voor de tijdelijke inschrijving van het voertuig);
- de datum van de laatste inschrijving van het voertuig;
- het koetswerktype van het voertuig;
- de cilinderinhoud (in cm^3) van het voertuig;
- het brandstoftype of de vermogensbron van het voertuig;

---

[8] Het betreft het adres van zijn hoofdverblijfplaats of, in het geval van een aan de gang zijnde procedure tot het bekomen van een verblijfsvergunning in België, het adres van zijn voorlopige verblijfplaats.

[9] Het stelt zich wel de vraag of het gegeven "adres" niet beter bij het Rijksregister wordt opgevraagd, daar dit ter zake de authentieke bron betreft.

- de milieuklasse van de EG-goedkeuring (vermelding van toepasselijke versie) van het voertuig;
- naam, adres en in voorkomend geval codenummer van de verzekeringsonderneming die het risico van de burgerrechtelijke aansprakelijkheid van de eigenaar of van de gebruiker van het voertuig dekt.

24. Het Comité merkt vooreerst op dat het slechts bevoegd is voor zover het om persoonsgegevens gaat[10]. Gegevens met betrekking tot een rechtspersoon zijn bijvoorbeeld geen persoonsgegevens.

25. In de mate dat het om persoonsgegevens gaat, beslist het Comité dat bovenstaande gegevens ter zake dienend, toereikend en niet overmatig zijn in het licht van de vooropgestelde doeleinden.

26. Ten tweede stelt het Comité vast dat alle personen die toegang vragen tot deze gegevens, ook het rijksregisternummer van de betrokkenen zullen ontvangen. Het Comité is niet bevoegd om te beoordelen of het gebruik van het rijksregisternummer door elke vragende instantie in deze gerechtvaardigd is. Het stelt vast dat er ter zake reeds een aantal machtigingen werden verleend:

- koninklijk besluit van 30 september 1985 *waarbij aan de onderzoeksrechters, aan de magistraten van het openbaar ministerie, aan de hoofdsecretarissen, aan de secretarissen-hoofden van dienst, aan de secretarissen, aan de adjunct-secretarissen en aan de opstellers die personeelslid zijn van de parketten, van de arbeidsauditoraten of van de krijgsauditoraten, toegang wordt verleend tot het Rijkregister van de natuurlijke personen en zij gemachtigd worden het identificatienummer van het Rijksregister van de natuurlijke personen aan te wenden;*

- koninklijk besluit van 14 maart 1991 *waarbij aan de griffiers van de hoven en rechtbanken van de Rechterlijke Orde toegang wordt verleend tot het Rijksregister van de natuurlijke personen en zij gemachtigd worden het identificatienummer van het Rijksregister van de natuurlijke personen aan te wenden;*

- koninklijk besluit van 15 oktober 2001 *waarbij de Veiligheid van de Staat gemachtigd wordt om het identificatienummer van het Rijksregister van de natuurlijke personen te gebruiken.*

27. Het Comité stelt zich evenwel de vraag of deze machtigingen volstaan opdat het gebruik van het Rijksregisternummer in deze context kan gerechtvaardigd worden. Gelet op het feit dat het

---

[10] Cf. supra randnummer 6.

hiervoor zelf niet bevoegd is, verzoekt het Comité het Sectoraal Comité voor het Rijksregister om in deze een standpunt in te nemen. Ingeval een bijkomende machtiging noodzakelijk is voor het gebruik van het Rijksregisternummer, dan zal de FOD Justitie hiervan op de hoogte worden gebracht.

28. Het Comité vestigt er ten derde de aandacht op dat de ingewonnen gegevens beschouwd worden als zijnde gerechtelijke gegevens zoals bedoeld in artikel 8 van de WVP aangezien zij worden verzameld om gebruikt te worden in een gerechtelijke procedure. Bijgevolg gelden in deze strengere modaliteiten.

29. Voornoemde voorwaarden staan vermeld in artikel 25 van het koninklijk besluit van 13 februari 2001 houdende uitvoering van de WVP (hierna KB van 13 februari 2001). Krachtens dit artikel moet de verantwoordelijke duidelijk de categorieën personen aanduiden die toegang hebben tot de gegevens en hun functie moet daarbij nauwkeurig worden omschreven. De lijst van de categorieën personen moet ter beschikking worden gehouden van de Commissie voor de bescherming van de persoonlijke levenssfeer (hierna "de Commissie"). Het KB van 13 februari 2001 verplicht de verantwoordelijke voor de verwerking (in casu de FOD Justitie) met andere woorden om een gepast toegangsbeheerssysteem te creëren en te handhaven. Het Comité staat er op dat hier werk van gemaakt wordt.

30. De verantwoordelijke moet er bovendien over waken dat de personen die toegang krijgen tot de gegevens gebonden zijn aan een wettelijke, statutaire of contractuele verplichting aangaande de vertrouwelijkheid van de gegevens. Wat deze voorwaarde betreft kan worden opgemerkt dat in een strafonderzoek – en dit zowel in het opsporingsonderzoek[11] als in het gerechtelijk onderzoek[12] – een onderzoeksgeheim geldt. Eenieder die beroepshalve zijn medewerking verleent aan het strafonderzoek is erdoor gehouden. Deze plicht heeft aldus een ruime draagwijdte en rust onder meer op magistraten, griffiers, stagiairs en andere medewerkers. Verder kan ook worden verwezen naar artikel 458 van het Strafwetboek op grond waarvan *"(...) personen die uit hoofde van hun staat of beroep kennis dragen van geheimen die hun zijn toevertrouwd (...)"* strafrechtelijk kunnen gesanctioneerd worden wanneer zij deze geheimen bekendmaken (behoudens een aantal uitzonderingen). Tot slot kan ook de discretieplicht in de zin van artikel 10 van het koninklijk besluit van 2 oktober 1937 *houdende het statuut van het rijkspersoneel* worden aangehaald.

---

[11] Artikel 28*quinquies*, § 1 van het Wetboek van Strafvordering.

[12] Artikel 57 van het Wetboek van Strafvordering.

2.2. Bewaringstermijn van de gegevens

31. Aangaande de bewaringstermijn van de gegevens herinnert het Comité er aan dat de gegevens niet langer bewaard mogen worden dan nodig voor het realiseren van de doeleinden waarvoor ze werden ingezameld (artikel 4, § 1, 5°, WVP).

32. In verband met de bewaringstermijn van de informatie afkomstig van de DIV, verwijst de FOD Justitie naar de Archiefwet van 24 juni 1955:

> *"Art. 1. Archiefdocumenten van meer dan dertig jaar oud, bewaard door de rechtbanken van de rechterlijke macht, (...), de Rijksbesturen, (...) worden, behoudens regelmatige vrijstelling, in goede, geordende en toegankelijke staat naar het Rijksarchief overgebracht. (...)*
>
> *Art. 2. De in het Rijksarchief berustende archiefstukken mogen niet worden vernietigd zonder toestemming van de verantwoordelijke overheid (...) die de overbrenging verricht heeft. (...)*
>
> *Art. 5. De overheden, bedoeld in het eerste artikel, (...) mogen geen archiefdocumenten vernietigen zonder toestemming van de algemene rijksarchivaris of van diens gemachtigde."*

33. Het Comité neemt hier akte van. Het is evenwel van oordeel dat in de praktijk een onderscheid kan gemaakt worden tussen verschillende bewaringswijzen. De behandeling van een hangend dossier vereist een bewaring van gegevens opdat deze op normale wijze beschikbaar en toegankelijk zouden zijn voor de ambtenaren die belast zijn met het beheer van het dossier. Zodra een dossier kan worden gearchiveerd, moet de gekozen bewaringswijze aan de gegevens slechts een beperkte beschikbaarheid en toegankelijkheid verlenen. Eens de bewaring niet langer nuttig is, dienen de gegevens niet langer te worden bewaard.

2.3. Frequentie van de toegang en de duur van machtiging

34. Aldus de FOD Justitie hebben de magistraten nood aan de gevraagde gegevens bij de DIV, telkens wanneer er *"een gerechtelijke opdracht de consultatie vereist"*. De ambtenaren van de FOD Justitie die werkzaam zijn bij de Centrale Autoriteit Internationale Samenwerking in Strafzaken hebben eveneens een permanente toegang nodig, opdat zij ten allen tijde zouden kunnen antwoorden op vragen van buitenlandse gerechtelijke autoriteiten. Hetzelfde geldt voor de medewerkers van de Veiligheid van de Staat: gelet op de opdrachten van deze dienst (cf. supra randnummer 13) is een permanente toegang eveneens aangewezen.

35. Gelet op wat vooraf gaat is het Comité van oordeel dat de gevraagde <u>permanente</u> toegang in deze noodzakelijk en gepast is in het licht van artikel 4, § 1, 3°, WVP.

36. De toegang wordt ook voor onbepaalde duur gevraagd en het Comité is van oordeel dat dit gepast is in het licht van de vooropgestelde doeleinden.

2.4. Bestemmelingen en/of derden waaraan gegevens worden meegedeeld

37. Het Comité stelt vast dat de volgende personen toegang zullen hebben tot de gevraagde gegevens:

- magistraten (zowel leden van de staande als van de zittende magistratuur);
- medewerkers van magistraten;
- ambtenaren van de FOD Justitie die werkzaam zijn bij de Centrale Autoriteit Internationale Samenwerking in Strafzaken;
- de applicatiebeheerders en systeembeheerders binnen de Stafdienst ICT (Directie Infrastructuur) van de FOD Justitie;
- medewerkers van de Veiligheid van de Staat.

38. Het Comité ziet in het licht van artikel 4, § 1, 3° WVP geen bezwaren tegen het feit dat bovengenoemde personen toegang hebben tot onderhavige persoonsgegevens, op voorwaarde dat zij enkel van deze toegang gebruik maken binnen de perken van de taken en bevoegdheden die hen werden toegekend. Het verwijst ter zake nogmaals naar de beperkingen die het in randnummer 11 heeft opgelegd. Het verzoekt ook om de nodige maatregelen te nemen opdat enkel die personen toegang kunnen krijgen en het wijst nogmaals op de bijzondere voorwaarden vervat in artikel 25 van het KB van 13 februari 2001 (cf. supra randnummers 28-30).

3. TRANSPARANTIEBEGINSEL

39. Het Comité herinnert eraan dat een eerlijke verwerking van gegevens een verwerking is die gebeurt op een transparante wijze. Eén van de hoekstenen van een transparante verwerking, betreft de informatieplicht in de zin van artikel 9, § 2, WVP.

40. De gegevensverwerkingen die worden uitgevoerd door de Veiligheid van de Staat zijn evenwel vrijgesteld van dergelijke verplichting (artikel 3, § 4 , WVP).

41. De andere gegevensverwerkingen die in onderhavig dossier worden voorgesteld, zullen verricht worden met het oog op de toepassing van bepalingen voorgeschreven door of krachtens een wet, een decreet of een ordonnantie. Op grond van artikel 9, § 2, 2de lid, b), WVP is in een dergelijke situatie een vrijstelling van de informatieplicht van kracht. Deze vrijstelling neemt echter

niet weg dat het Comité er zich kan van vergewissen of er passende waarborgen bestaan voor de bescherming van de fundamentele rechten van de betrokkenen.

42. Vanuit die optiek beveelt het Comité aan dat de DIV op haar website zou vermelden dat haar repertorium toegankelijk is voor de rechterlijke macht en voor de Centrale Autoriteit Internationale Samenwerking In Strafzaken.

4. BEVEILIGING

4.1. Op het niveau van de FOD Justitie

43. Uit de door de FOD Justitie meegedeelde stukken blijkt dat hij over een veiligheidsconsulent beschikt en dat zijn geschreven veiligheidsbeleid tegen uiterlijk eind 2010 zal gefinaliseerd zijn. Het Comité heeft hier akte van genomen.

4.2. Op het niveau van de DIV

44. Het Comité vestigt de aandacht op het feit dat elke beveiligde gegevensstroom vereist dat aan beide zijden veiligheidsmaatregelen worden genomen, dus ook door de DIV. Met betrekking tot dit aspect van de beveiliging kan het Comité zich evenwel niet uitspreken vermits hierover geen enkele informatie werd verstrekt. Een evaluatievragenlijst met verwijzing naar de door de Commissie gepubliceerde "Referentiemaatregelen voor de beveiliging van elke verwerking van persoonsgegevens" dient dan ook door deze instelling te worden ingevuld en naar het Comité te worden gestuurd.

OM DEZE REDENEN,

het Comité

machtigt de FOD Justitie en de DIV om de verwerkingen bedoeld in de aanvraag, uit te voeren, mits rekening wordt gehouden met de hierboven geschetste opmerkingen (zie in het bijzonder randnummers 11, 14, 26-27, 28-30, 33, 38, 42 en 44).

Voor de Administrateur m.v., De Voorzitter,

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

Comité sectoriel pour l'Autorité Fédérale

Délibération AF n° 23/2010 du 21 décembre 2010

Objet : demande d'autorisation pour le traitement de données de la DIV par le SPF Justice et les instances judiciaires (AF/MA/2010/123)

Le Comité sectoriel pour l'Autorité Fédérale (ci-après "le Comité") ;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après "la LVP"), en particulier les articles 31*bis* et 36*bis* ;

Vu l'arrêté royal du 17 décembre 2003 *fixant les modalités relatives à la composition et au fonctionnement de certains comités sectoriels institués au sein de la Commission de la protection de la vie privée*, en particulier l'article 18 ;

Vu la demande de Monsieur A. Bourlet, Président du Comité de direction du Service public fédéral Justice, reçue le 03/11/2010 ;

Vu la demande d'avis technique et juridique adressée au Service public fédéral Fedict en date du 02/12/2010 ;

Vu l'avis technique et juridique reçu le 16/12/2010 ;

Vu le rapport du Président ;

Émet, après délibération, la décision suivante, le 21/12/2010:

I. OBJET ET CONTEXTE DE LA DEMANDE

1. Dans sa demande d'autorisation du 3 novembre 2010, le SPF Justice demande au Comité l'obtention d'un accès au répertoire des véhicules de la Direction pour l'Immatriculation des Véhicules du Service public fédéral Mobilité et Transports (ci-après "la DIV"). Cette demande a été complétée par des informations complémentaires les 30 novembre 2010 et 1er décembre 2010.

2. Les données demandées seront utilisées par trois instances différentes :

- le pouvoir judiciaire ;
- l'Autorité centrale de coopération internationale en matière pénale (une entité du SPF Justice) ;
- la Sûreté de l'État (également une entité du SPF Justice).

3. Actuellement, les instances précitées disposent déjà d'un accès aux informations demandées. Suite à l'instauration d'une nouvelle technologie (une structure server-to-server) pour rendre cet accès plus opérationnel à l'avenir, le SPF Justice et la DIV ont décidé d'également introduire une demande auprès du Comité afin de se mettre en règle avec l'article 36*bis* de la LVP.

II. EXAMEN DE LA DEMANDE

A. COMPÉTENCE DU COMITÉ

4. En vertu de l'article 36*bis* de la LVP, "*toute communication électronique de données personnelles par un service public fédéral ou par un organisme public avec personnalité juridique qui relève de l'autorité fédérale, exige une autorisation de principe* (du comité sectoriel compétent)".

5. Il incombe à ce Comité de vérifier "*que ladite communication, d'une part, est nécessaire à la mise en œuvre des missions confiées, par ou en vertu de la loi, à l'autorité fédérale demanderesse et, d'autre part, que cette communication, en ses divers aspects, est compatible avec l'ensemble des normes en vigueur en matière de protection de la vie privée en ce qui concerne le traitement de données personnelles.*" (Doc. Parl. 50, 2001-2002, n° 1940/004).

6. La DIV, qui fait partie du SPF Mobilité et Transports, transmettra par voie électronique des données au SPF Justice. Dans la mesure où les données échangées concernent des données à

caractère personnel[1], le Comité est dès lors compétent pour se prononcer sur cette communication électronique.

B. QUANT AU FOND

1. PRINCIPE DE FINALITÉ

7. L'article 4, § 1, 2° de la LVP n'autorise le traitement de données à caractère personnel que pour des finalités déterminées, explicites et légitimes et les données ne peuvent en outre pas être traitées ultérieurement de manière incompatible avec ces finalités. Le Comité examine dans les paragraphes qui suivent si ces principes sont respectés dans le cas présent.

8. Le Comité déduit de la demande que l'accès demandé vise trois finalités différentes :

- l'exécution des missions de la magistrature (ci-après "la première finalité") ;
- la communication du titulaire de l'immatriculation d'un véhicule à des autorités judiciaires étrangères par l'Autorité centrale de coopération internationale en matière pénale (ci-après "la deuxième finalité") ;
- les missions de certains agents de la Sûreté de l'État (ci-après "la troisième finalité").

9. En ce qui concerne la première finalité, la demande attire l'attention sur les larges compétences de la magistrature et donne une description générale des finalités visées par l'accès qui est demandé :

> "*Concernant l'arbitrage des contestations, le pouvoir judiciaire a une compétence qui n'est limitée que par la prescription constitutionnelle selon laquelle le législateur peut retirer au Pouvoir les contestations sur les droits politiques qu'il a définis (lisez surtout les affaires administratives). Cela signifie que, sauf dans les cas exceptionnels, toutes les contestations possibles concernant tous les sujets possibles peuvent être soumises à l'arbitrage des cours et tribunaux[2]. (...) Il résulte de ce qui précède qu'il n'est pas possible d'énumérer précisément les contestations dont le Pouvoir judiciaire prend connaissance ou de les définir. Une telle énumération ou définition présenterait de grandes lacunes, tant au moment où elle est effectuée que d'un point de vue diachronique car rapidement, elle ne serait plus adéquate en raison de l'évolution permanente de la société. (...)*

[1] La demande concerne aussi des données relatives à des personnes morales. Il ne s'agit pas de données à caractère personnel au sens de l'article 1, § 1 de la LVP (cf. les points 23-24).

[2] Voir également les articles 144 et 145 de la Constitution.

Lorsque, pour l'arbitrage d'une contestation quelconque pour laquelle il est compétent, le Pouvoir judiciaire a besoin de données liées à un véhicule, il doit pouvoir connaître ces données, au risque sinon de ne pas pouvoir exécuter correctement sa mission constitutionnelle et légale. Cela aurait la même conséquence qu'un déni de justice pour défaut d'arbitrage ou pour arbitrage erroné. (...)
La finalité de l'utilisation des données du répertoire est d'obtenir des informations aussi exactes que possible dans le cadre de l'arbitrage des contestations pour lesquelles le Pouvoir judiciaire est compétent, afin de garantir la qualité de cet arbitrage des contestations et ainsi de garantir le respect des droits de toutes les parties concernées." [Traduction libre réalisée par le secrétariat de la Commission, en l'absence d'une traduction officielle].

10. La demande ajoute que la consultation sera généralement effectuée par les parquets (les magistrats du ministère public) et les juges d'instruction ainsi que les collaborateurs qu'ils auront désignés (les secrétaires du parquet, les greffiers et les membres du personnel du parquet et du greffe). En outre, selon le SPF Justice, cela favorisera la procédure si les magistrats des juridictions de jugement et les magistrats des tribunaux civils ainsi que les collaborateurs qu'ils ont désignés (les greffiers et le personnel du greffe) peuvent consulter le répertoire afin de contrôler l'exactitude des données fournies par les parties en litige ou d'autres personnes concernées par le procès.

11. Concernant la première finalité, le Comité souscrit au point de vue du SPF Justice, à savoir qu'il n'est pas possible de donner une énumération détaillée et exhaustive des cas où le pouvoir judiciaire souhaite un accès aux données demandées. Il décide que la définition qui est citée au point 9 suffit pour qu'il soit question de finalités déterminées et explicites au sens de l'article 4, § 1, 2° de la LVP. Toutefois, il s'interroge sérieusement quant à la proposition d'octroyer un accès à tous les membres de la magistrature assise ainsi qu'à tous les collaborateurs qui ont été désignés par des magistrats. Le Comité ne voit aucune justification raisonnable pour un accès aussi large et décide de limiter celui-ci :

- à la magistrature debout ;
- à la magistrature assise, pour autant que les magistrats qui consultent les données de la DIV le fassent dans le cadre d'une mission d'investigation telle que définie dans le Code d'instruction criminelle, le Code judiciaire et/ou les lois spéciales ;
- aux collaborateurs des magistrats, pour autant qu'ils ne consultent les données de la DIV que dans le cadre des missions qui leur ont été confiées par la législation.

12. Quant à la deuxième finalité, la demande précise que les données seront transmises à des autorités judiciaires étrangères dans les cas où des infractions au code de la route ou d'autres délits

sont commis dans leur pays avec des véhicules immatriculés à la DIV. Le Comité estime qu'il s'agit également d'une finalité déterminée et explicite.

13. En ce qui concerne la troisième finalité, le Comité en arrive aussi à la même conclusion. Les collaborateurs habilités utiliseront en effet cet accès dans le cadre de la réalisation des missions de la Sûreté de l'État, à savoir :

> "*La Sûreté de l'État a pour mission :*
> *1° de rechercher, d'analyser et de traiter le renseignement relatif à toute activité qui menace ou pourrait menacer la sûreté intérieure de l'État et la pérennité de l'ordre démocratique et constitutionnel, la sûreté extérieure de l'État et les relations internationales, le potentiel scientifique ou économique défini par le Comité ministériel, ou tout autre intérêt fondamental du pays défini par le Roi sur proposition du Comité ministériel ;*
> *2° d'effectuer les enquêtes de sécurité qui lui sont confiées conformément aux directives du Comité ministériel ;*
> *3° d'exécuter les tâches qui lui sont confiées par le Ministre de l'Intérieur en vue de protéger des personnes ;*
> *4° d'exécuter toutes autres missions qui lui sont confiées par ou en vertu de la loi.*"[3]

14. Le Comité attire l'attention sur le fait que les données demandées ne peuvent être utilisées que pour les trois finalités énumérées dans la demande d'autorisation (cf. le point 8 ci-dessus).

15. Concernant l'exigence de compatibilité avec la finalité initiale, le Comité signale que les traitements envisagés, à savoir la transmission de certaines données par la DIV aux trois instances susmentionnées, constituent des traitements ultérieurs de données traitées initialement pour d'autres finalités. La licéité de ces traitements ultérieurs dépend donc de leur compatibilité avec le traitement initial. L'examen de la compatibilité se fait en fonction des prévisions raisonnables de l'intéressé et des dispositions légales et réglementaires applicables.

16. À cet égard, concernant la première finalité, le Comité constate que :

- les articles 144 et 145 de la Constitution stipulent ce qui suit :
  "*Art. 144. Les contestations qui ont pour objet des droits civils*[4] *sont exclusivement du ressort des tribunaux.*

---

[3] Article 7 de la *loi organique des services de renseignement et de sécurité* du 30 novembre 1998.

[4] Au sens constitutionnel du terme, "contestations qui ont pour objet des droits civils" signifient toutes les contestations qui ne concernent pas les droits politiques. Les affaires criminelles font également partie de ces contestations qui ont pour objet des droits civils.

Art. 145. Les contestations qui ont pour objet des droits politiques sont du ressort des tribunaux, sauf les exceptions établies par la loi."

- l'article 6 de l'arrêté royal du 20 juillet 2001 *relatif à l'immatriculation de véhicules* (ci-après l'arrêté royal du 20 juillet 2001) stipule ce qui suit :
  "*Art. 6. (...)*
  § 2. Les finalités pour lesquelles les données à caractère personnel du répertoire peuvent faire l'objet d'un traitement sont :
  1° la recherche et la poursuite pénale des crimes, délits et contraventions ; (...)
  10° la saisie conservatoire et la saisie-exécution des véhicules à moteur et des remorques ;
  11° la police de la circulation routière et de la sécurité routière, la sécurité des véhicules à moteur et des remorques incluses ; (...)
  15° le contrôle de la couverture en responsabilité civile à laquelle peuvent donner lieu les véhicules à moteur et remorques ;
  16° la communication aux personnes impliquées dans un accident de la circulation routière, du nom des compagnies d'assurance couvrant la responsabilité civile résultant de l'utilisation de chacun des véhicules concernés par cet accident ; (...)"[5].

17. Le Comité constate donc qu'en ce qui concerne la première finalité, il existe un cadre réglementaire suffisamment clair pour garantir un traitement ultérieur compatible.

18. Concernant la deuxième finalité, le Comité constate que :

- l'article 3, premier alinéa de la *Convention européenne d'entraide judiciaire en matière pénale* du 20 avril 1959 stipule ce qui suit :
  "*La Partie requise fera exécuter, dans les formes prévues par sa législation, les commissions rogatoires relatives à une affaire pénale qui lui seront adressées par les autorités judiciaires de la Partie requérante et qui ont pour objet d'accomplir des actes d'instruction ou de communiquer des pièces à conviction, des dossiers ou des documents.*"

- l'article 53 de la *Convention du 19 juin 1990 d'application de l'Accord de Schengen du 14 juin 1985 entre les gouvernements des États de l'Union économique Benelux, de la République fédérale d'Allemagne et de la République française relatif à la suppression graduelle des contrôles aux frontières communes* stipule ce qui suit :

[5] Par ailleurs, le Comité constate également que la loi du 19 mai 2010 *portant création de la Banque-Carrefour des véhicules* (M.B. du 28 juin 2010) prévoit des règles similaires (cf. article 5, 7°, 16°, 17°, 21°, 22° de cette loi). Cette loi n'est toutefois pas encore entrée en vigueur (cf. article 40).

"*1. Les demandes d'entraide judiciaire peuvent être faites directement entre les autorités judiciaires et renvoyées par la même voie.*
2. Le paragraphe 1 ne porte pas préjudice à la faculté de l'envoi et du renvoi des demandes de Ministère de la Justice à Ministère de la Justice ou par l'intermédiaire des bureaux centraux nationaux de l'Organisation Internationale de Police Criminelle."

- l'article 6 de l'arrêté royal du 20 juillet 2001 stipule ce qui suit :
"*Art. 6. (...)*
§ 2. Les finalités pour lesquelles les données à caractère personnel du répertoire peuvent faire l'objet d'un traitement sont :
1° la recherche et la poursuite pénale des crimes, délits et contraventions ; (...)
10° la saisie conservatoire et la saisie-exécution des véhicules à moteur et des remorques ;
11° la police de la circulation routière et de la sécurité routière, la sécurité des véhicules à moteur et des remorques incluses ; (...)"[6].

19. Le Comité constate donc qu'en ce qui concerne la deuxième finalité, il existe également un cadre réglementaire suffisamment clair pour garantir un traitement ultérieur compatible.

20. Concernant la troisième finalité, le Comité constate que :

- l'article 14 de la *loi organique des services de renseignement et de sécurité* du 30 novembre 1998 stipule ce qui suit :
"*(...) Dans le respect de la législation en vigueur, les services de renseignement et de sécurité peuvent selon les modalités générales fixées par le Roi, avoir accès aux banques de données du secteur public utiles à l'exécution de leurs missions.*"

- les articles 3 et 4 de l'arrêté royal du 12 octobre 2010 *portant exécution de diverses dispositions de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité*[7] stipulent ce qui suit :
"*Art. 3. § 1er. Pour l'application de l'article 14, alinéa 4, de la loi du 30 novembre 1998, lorsque les services de renseignement et de sécurité peuvent disposer d'un accès direct à une banque de données du secteur public contenant des données à caractère personnel, le dirigeant du service concerné tient en permanence à la disposition de la Commission de la*

[6] Par ailleurs, le Comité constate également que la loi du 19 mai 2010 *portant création de la Banque-Carrefour des véhicules* (M.B. du 28 juin 2010) prévoit des règles similaires (cf. article 5, 7°, 16°, 17° de cette loi). Cette loi n'est toutefois pas encore entrée en vigueur (cf. article 40).

[7] Voir également l'avis favorable de la Commission de la protection de la vie privée (n° 24/2010 du 30 juin 2010) lorsque cet arrêté royal était encore en préparation.

protection de la vie privée la liste nominative des personnes habilitées à accéder à la banque de données, avec indication de leur titre et de leur fonction.
L'identité des auteurs de toute demande de consultation d'une banque de données est enregistrée dans un système de contrôle au sein du service de renseignement et de sécurité concerné. Ces informations sont conservées pendant dix ans. (...)
Art. 4. § 1er. Un conseiller en sécurité de l'information et en protection de la vie privée, qui remplit, entre autres, la fonction de préposé à la protection des données, visé à l'article 17bis de la loi du 8 décembre 1992, est désigné au sein de chaque service de renseignement et de sécurité, par le ministre compétent, sur la proposition du dirigeant du service concerné.
Il est placé sous l'autorité directe du dirigeant du service auquel il rend des comptes et fait rapport exclusivement. Il est chargé de manière indépendante :
- de garantir le respect de la loi lors de toute demande de données ;
- de prendre toutes mesures utiles afin d'assurer la sécurité des informations enregistrées ;
- de fournir des avis qualifiés au dirigeant du service ;
- d'exécuter d'autres missions qui lui sont confiées par le dirigeant du service.
Le conseiller en sécurité de l'information et en protection de la vie privée, visé à l'alinéa 1er, peut se faire assister par un ou plusieurs adjoints.
§ 2. En ce qui concerne la Sûreté de l'État, la fonction de conseiller en sécurité de l'information et en protection de la vie privée, qui remplit, entre autres, la fonction de préposé à la protection des données, visé au § 1er, est exercée par le conseiller à la sécurité des données désigné par le Ministre de la Justice, conformément à l'article 6 de l'arrêté royal du 28 février 2002 relatif à la transmission d'informations par les communes, à la Sûreté de l'État, par l'intermédiaire du Registre national des personnes physiques."

21. Le Comité constate donc qu'en ce qui concerne la dernière finalité, il existe également un cadre réglementaire suffisamment clair pour garantir un traitement ultérieur compatible.

2. PRINCIPE DE PROPORTIONNALITÉ

2.1. Nature des données

22. L'article 4, § 1, 3° de la LVP stipule que les données à caractère personnel doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement.

23. Le SPF Justice affirme dans sa demande que, pour réaliser les finalités telles que définies au point 8, la magistrature, l'Autorité centrale de coopération internationale en matière pénale et la Sûreté de l'État doivent pouvoir consulter les données suivantes :

- le nom, le prénom, la date de naissance, le numéro de Registre national et l'adresse[8] [9] de la personne au nom de laquelle le véhicule est immatriculé ;
- l'adresse de la résidence provisoire des personnes visées à l'article 5, § 1er, 1° et 2° de l'arrêté royal du 20 juillet 2001 ;
- le nom, la forme juridique et le numéro de TVA de la personne morale au nom de laquelle le véhicule est immatriculé ;
- le numéro d'immatriculation (le numéro de la plaque minéralogique) du véhicule ;
- la date de la première immatriculation du véhicule (en Belgique ou à l'étranger) ;
- la marque ou, si la marque n'est pas connue, le nom du constructeur du véhicule ;
- le type et, le cas échéant, la variante et la version concernant ce type de véhicule ;
- la dénomination commerciale du véhicule ;
- le numéro d'identification (numéro de châssis) du véhicule ;
- la durée de validité de l'immatriculation (uniquement pour l'immatriculation provisoire du véhicule) ;
- la date de la dernière immatriculation du véhicule ;
- le type de carrosserie du véhicule ;
- la cylindrée (en cm^3) du véhicule ;
- le type de carburant ou la source d'énergie du véhicule ;
- la classe environnementale de l'homologation CE (mention de la version applicable) du véhicule ;
- le nom, l'adresse et, le cas échéant, le numéro de code de la compagnie d'assurances qui couvre le risque de responsabilité civile du propriétaire ou de l'usager du véhicule.

24. Tout d'abord, le Comité fait remarquer qu'il n'est compétent que pour autant qu'il s'agisse de données à caractère personnel[10]. Les données relatives à une personne morale, par exemple, ne sont pas des données à caractère personnel.

[8] Il s'agit de l'adresse de sa résidence principale ou, dans le cas d'une procédure en cours pour l'obtention d'un permis de séjour en Belgique, de l'adresse de sa résidence provisoire.

[9] La question se pose néanmoins de savoir s'il ne serait pas préférable de réclamer "l'adresse" auprès du Registre national, étant donné qu'il constitue la source authentique en la matière.

[10] Cf. le point 6 ci-dessus.

25. Dans la mesure où il s'agit de données à caractère personnel, le Comité décide que les données susmentionnées sont pertinentes, adéquates et non excessives à la lumière des finalités envisagées.

26. Deuxièmement, le Comité constate que toutes les personnes qui demandent un accès à ces données recevront également le numéro de Registre national des personnes concernées. Le Comité n'est pas compétent pour juger si l'utilisation du numéro de Registre national par chaque instance demandeuse est légitime dans ce cas. Il constate qu'en la matière, plusieurs autorisations ont déjà été accordées :

- l'arrêté royal du 30 septembre 1985 *autorisant les juges d'instruction, les magistrats du ministère public, les secrétaires en chef, les secrétaires chefs de service, les secrétaires, les secrétaires adjoints et les rédacteurs membres du personnel des parquets, des auditorats du Travail ou Militaires, à accéder au Registre national des personnes physiques et à utiliser le numéro d'identification du Registre national des personnes physiques* ;

- l'arrêté royal du 14 mars 1991 *autorisant les greffiers des cours et tribunaux de l'Ordre judiciaire à accéder au Registre national des personnes physiques et à utiliser le numéro d'identification du registre national des personnes physiques* ;

- l'arrêté royal du 15 octobre 2001 *autorisant la Sûreté de l'État à utiliser le numéro d'identification du Registre national des personnes physiques.*

27. Le Comité se demande toutefois si ces autorisations suffisent pour pouvoir légitimer l'utilisation du numéro de Registre national dans ce contexte. Vu qu'il n'est pas lui-même compétent pour en juger, le Comité demande au Comité sectoriel du Registre national d'adopter un point de vue à cet égard. Si une autorisation complémentaire est nécessaire pour l'utilisation du numéro de Registre national, le SPF Justice en sera informé.

28. Troisièmement, le Comité attire l'attention sur le fait que les données recueillies sont considérées comme des données judiciaires telles que visées à l'article 8 de la LVP étant donné qu'elles sont collectées pour être utilisées dans une procédure judiciaire. Dès lors, des modalités plus strictes s'appliquent en la matière.

29. Les conditions précitées sont mentionnées à l'article 25 de l'arrêté royal du 13 février 2001 portant exécution de la LVP (ci-après l'arrêté royal du 13 février 2001). En vertu de cet article, le responsable doit clairement désigner les catégories de personnes qui ont accès aux données, avec une description précise de leur fonction. La liste des catégories de personnes doit être tenue à la

disposition de la Commission de la protection de la vie privée (ci-après "la Commission"). L'arrêté royal du 13 février 2001 oblige en d'autres termes le responsable du traitement (en l'occurrence le SPF Justice) à créer et mettre en application un système adéquat de gestion des accès. Le Comité insiste pour que le SPF Justice s'y attelle.

30. Le responsable doit en outre veiller à ce que les personnes ayant accès aux données soient tenues, par une obligation légale, statutaire ou contractuelle, de respecter la confidentialité des données. En ce qui concerne cette condition, on peut préciser que lors d'une enquête pénale – et ce aussi bien lors de l'information[11] que lors de l'instruction[12] – le secret de l'instruction est d'application. Toute personne qui offre à titre professionnel sa collaboration à l'enquête pénale y est tenue. Cette obligation a donc une large portée et repose notamment sur les magistrats, les greffiers, les stagiaires et les autres collaborateurs. De plus, on peut également attirer l'attention sur l'article 458 du Code pénal en vertu duquel "*(...) toutes autres personnes dépositaires, par état ou par profession, des secrets qu'on leur confie(...)*" peuvent être sanctionnées pénalement lorsqu'elles révèlent ces secrets (sauf plusieurs exceptions). Enfin, le devoir de discrétion au sens de l'article 10 de l'arrêté royal du 2 octobre 1937 *portant le statut des agents de l'État* peut également être cité.

2.2. Délai de conservation des données

31. En ce qui concerne le délai de conservation des données, le Comité rappelle que les données doivent être conservées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues (article 4, § 1, 5° de la LVP).

32. Concernant le délai de conservation des informations provenant de la DIV, le SPF Justice se réfère à la loi sur les archives du 24 juin 1955 :

> *"Article 1. Les documents datant de plus de trente ans conservés par les tribunaux de l'ordre judiciaire, (...), les administrations de l'État (...) sont déposés - sauf dispense régulièrement accordée - en bon état, ordonnées* [Note de la traduction : lire "ordonnés"] *et accessibles aux Archives de l'État.*
> *(...)*
> *Art. 2. Les documents reposant aux Archives de l'État ne peuvent être détruits sans le consentement des autorités responsables (...) qui en a opéré le transfert.*
> *Art. 5. Les autorités visées à l'article 1er (...) ne pourront procéder à la destruction de documents sans avoir obtenu l'autorisation de l'archiviste général du Royaume ou de ses délégués.*"

[11] Article 28*quinquies*, § 1 du Code d'instruction criminelle.
[12] Article 57 du Code d'instruction criminelle.

33. Le Comité en prend acte. Il estime toutefois que l'on peut faire une distinction en pratique entre différents modes de conservation. Le traitement d'un dossier pendant requiert une conservation de données de manière telle que celles-ci soient disponibles et accessibles normalement pour les fonctionnaires chargés de la gestion du dossier. Dès qu'un dossier peut être archivé, le mode de conservation choisi ne doit conférer aux données qu'une disponibilité et une accessibilité limitées. Une fois que la conservation n'est plus utile, les données ne doivent plus être conservées.

2.3. Fréquence de l'accès et durée de l'autorisation

34. Selon le SPF Justice, les magistrats ont besoin des données demandées auprès de la DIV chaque fois qu' "une mission judiciaire requiert la consultation". Les agents du SPF Justice qui travaillent au sein de l'Autorité centrale de coopération internationale en matière pénale ont également besoin d'un accès permanent afin de pouvoir à tout moment répondre à des questions d'autorités judiciaires étrangères. Il en va de même pour les collaborateurs de la Sûreté de l'État : vu les missions de ce service (cf. le point 13 ci-dessus), un accès permanent est également recommandé.

35. Compte tenu de ce qui précède, le Comité estime que l'accès permanent demandé est nécessaire et approprié en la matière, à la lumière de l'article 4, § 1, 3° de la LVP.

36. L'accès est également demandé pour une durée indéterminée et le Comité estime que cela est approprié à la lumière des finalités envisagées.

2.4. Destinataires et/ou tiers auxquels des données sont communiquées

37. Le Comité constate que les personnes suivantes auront accès aux données demandées :

- les magistrats (tant des membres de la magistrature debout que de la magistrature assise) ;
- les collaborateurs de magistrats ;
- les agents du SPF Justice qui travaillent au sein de l'Autorité centrale de coopération internationale en matière pénale ;
- les gestionnaires d'applications et les gestionnaires de systèmes au sein du Service d'encadrement ICT (Direction Infrastructure) du SPF Justice ;
- les collaborateurs de la Sûreté de l'État.

4.2. Au niveau de la DIV

44. Le Comité attire l'attention sur le fait que tout flux de données sécurisé requiert que des mesures de sécurité soient prises des deux côtés, donc également par la DIV. Concernant cet aspect de la sécurité, le Comité ne peut toutefois se prononcer étant donné qu'aucune information n'a été fournie à ce sujet. Un questionnaire d'évaluation renvoyant aux "Mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel" publiées par la Commission doit dès lors être complété par cette instance et être renvoyé au Comité.

PAR CES MOTIFS,

le Comité

autorise le SPF Justice et la DIV à effectuer les traitements visés dans le demande, moyennant la prise en considération des remarques formulées ci-dessus (voir en particulier les points 11, 14, 26-27, 28-30, 33, 38, 42 et 44).

Pour l'Administrateur e.c., Le Président,

(sé) Patrick Van Wouwe (sé) Willem Debeuckelaere