DOC 55 **2043/002**

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

7 septembre 2021

PROPOSITION DE RÉSOLUTION

relative à la lutte contre la cyberfraude utilisant des mules bancaires

AVIS DE L'AUTORITÉ DE PROTECTION DES DONNÉES N^O^ 136/2021 DU 24 AOÛT 2021

Voir:

Doc 55 **2043/ (2020/2021)**:
001: Proposition de résolution de MM. Freilich et Donné.

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

7 september 2021

VOORSTEL VAN RESOLUTIE

betreffende het bestrijden van cyberfraude via geldezels

ADVIES VAN DE GEGEVENSBESCHERMINGSAUTORITEIT NR. 136/2021 VAN 24 AUGUSTUS 2021

Zie:

Doc 55 **2043/ (2020/2021)**:
001: Voorstel van resolutie van de heren Freilich en Donné.

N-VA	:	*Nieuw-Vlaamse Alliantie*
Ecolo-Groen	:	*Ecologistes Confédérés pour l'organisation de luttes originales – Groen*
PS	:	*Parti Socialiste*
VB	:	*Vlaams Belang*
MR	:	*Mouvement Réformateur*
CD&V	:	*Christen-Democratisch en Vlaams*
PVDA-PTB	:	*Partij van de Arbeid van België – Parti du Travail de Belgique*
Open Vld	:	*Open Vlaamse liberalen en democraten*
Vooruit	:	*Vooruit*
cdH	:	*centre démocrate Humaniste*
DéFI	:	*Démocrate Fédéraliste Indépendant*
INDEP-ONAFH	:	*Indépendant - Onafhankelijk*

Abréviations dans la numérotation des publications:		*Afkorting bij de numering van de publicaties:*	
DOC 55 0000/000	*Document de la 55e législature, suivi du numéro de base et numéro de suivi*	*DOC 55 0000/000*	*Parlementair document van de 55e zittingsperiode + basisnummer en volgnummer*
QRVA	*Questions et Réponses écrites*	*QRVA*	*Schriftelijke Vragen en Antwoorden*
CRIV	*Version provisoire du Compte Rendu Intégral*	*CRIV*	*Voorlopige versie van het Integraal Verslag*
CRABV	*Compte Rendu Analytique*	*CRABV*	*Beknopt Verslag*
CRIV	*Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)*	*CRIV*	*Integraal Verslag, met links het defi nitieve integraal verslag en rechts het vertaald beknopt verslag van de toespraken (met de bijlagen)*
PLEN	*Séance plénaire*	*PLEN*	*Plenum*
COM	*Réunion de commission*	*COM*	*Commissievergadering*
MOT	*Motions déposées en conclusion d'interpellations (papier beige)*	*MOT*	*Moties tot besluit van interpellaties (beigekleurig papier)*

Autorité de protection des données
Gegevensbeschermingsautoriteit

Avis n° 136/2021 du 24 août 2021

Objet : Avis relatif à une proposition de résolution relative à la lutte contre la cyberfraude utilisant des mules bancaires (CO-A-2021-155)

Le Centre de Connaissances de l'Autorité de protection des données (ci-après "l'Autorité"), en présence de Mesdames Marie-Hélène Descamps et Alexandra Jaspar et de Messieurs Yves-Alexandre de Montjoye, Bart Preneel et Frank Robben ;

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier les articles 23 et 26 (ci-après la "LCA") ;

Vu le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la Directive 95/46/CE* (Règlement général sur la protection des données, ci-après le "RGPD") ;

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* (ci-après "la LTD") ;

Vu la demande d'avis de Madame Éliane Tillieux, Présidente de la Chambre des représentants, reçue le 15/07/2021 ;

Vu le rapport d'Alexandra Jaspar ;

Émet, le 24 août 2021, l'avis suivant :

I. OBJET DE LA DEMANDE

1. Madame Éliane Tillieux, Présidente de la Chambre des représentants, recueille l'avis de l'Autorité sur une proposition de résolution relative à la lutte contre la cyberfraude utilisant des mules bancaires.

2. La résolution précise que les cybercriminels qui extorquent de l'argent via Internet ont généralement recours à des "money mules" (mules bancaires). Afin de ne pas se faire prendre eux-mêmes en faisant verser l'argent directement sur leur propre compte, par exemple, les escrocs font appel à des "mules bancaires". Ces personnes prêtent leur compte bancaire et/ou leur carte bancaire ainsi que leur code pin contre rémunération. L'argent volé peut ainsi être dépensé en ligne, être transféré sur un autre compte bancaire en Belgique ou à l'étranger ou être retiré à un distributeur de billets. Souvent, seule la mule bancaire peut être identifiée et condamnée alors que les donneurs d'ordre restent hors de portée.

3. Selon la résolution, ceci résulte du fait que les banques ne disposent pas de moyens pour attaquer le mal à la racine. Pour pouvoir démanteler les réseaux criminels, les échanges de données entre les banques devraient être beaucoup plus nombreux, par analogie avec le Risk Warning System (système de prévention des risques) aux Pays-Bas. Ce système permet aux banques d'entamer des enquêtes entre elles en cas de blanchiment d'argent. Les auteurs de la résolution insistent pour que le gouvernement élabore un cadre légal qui permette aux institutions financières d'échanger des informations sur les comptes suspects et les transactions suspectes, en cas de soupçon de blanchiment d'argent, afin de faciliter le démantèlement d'un éventuel réseau criminel.

II. EXAMEN DE LA DEMANDE

4. L'Autorité attire l'attention sur le fait que la recherche de criminels relève des services publics mandatés à cet effet. De telles enquêtes s'accompagnent en effet d'une immixtion dans la vie privée. La question se pose de savoir s'il appartient bien à des entreprises commerciales telles que des banques, qui sont finalement concurrentes les unes des autres, d'entamer, de leur propre initiative, des enquêtes entre elles sur leurs clients concernant le blanchiment d'argent et donc de mener au fond une enquête sur des infractions pénales et d'échanger des données sur des personnes dans ce cadre. Cela va bien au-delà par exemple d'une obligation de notification de transactions suspectes aux autorités judiciaires compétentes qui mènent des enquêtes pénales avec les garanties y afférentes pour les personnes concernées. Il en résulte en outre que les banques impliquées dans l'enquête (finalité d'enquête) entrent en possession de plus d'informations sur un client que ce dont elles disposent dans le cadre de leur relation commerciale (finalité commerciale) avec lui. Dès lors, le risque que les "informations d'enquête" soient ensuite utilisées à des fins commerciales est considérable.

5. Si l'on envisage d'attribuer à des entreprises commerciales un "rôle d'enquêteur", il faut chercher au maximum à assurer la minimisation des données par des « privacy enhancing technologies ». On peut penser ici à la technique de "Private Set Intersection" permettant aux banques d'établir chacune une "liste noire" reprenant les noms ou comptes susceptibles d'être impliqués par des "money mules" (mules bancaires) et de vérifier ensuite quels noms figurent également sur la "liste noire" d'autres banques sans divulguer la moindre information sur des données qui n'apparaissent qu'une seule fois.

6. Tant que rien de précis n'a été élaboré, l'Autorité n'est pas en mesure d'établir un point de vue. Elle se voit dès lors contrainte de se limiter à rappeler ci-après les principes essentiels qui doivent être respectés lors de la rédaction éventuelle d'une réglementation.

A. Test de nécessité

7. Tout traitement de données à caractère personnel instauré par une réglementation implique en principe une limitation du droit à la protection des données à caractère personnel. Lors de la préparation d'un projet de texte normatif qui encadre des traitements de données à caractère personnel, il faut donc d'abord analyser si la mesure visée est bel et bien nécessaire pour atteindre l'objectif légitime qu'elle poursuit. Ce test de nécessité implique que l'auteur d'un projet de texte normatif réalise une analyse préalable d'une part des faits qui justifient l'instauration de la mesure et d'autre part du degré d'efficacité de la mesure à la lumière de la finalité qu'elle poursuit. Dans le cadre de cette analyse, l'auteur doit également vérifier si son objectif peut éventuellement être atteint via une mesure moins intrusive du point de vue de la protection des données.

B. Base juridique et prévisibilité de la norme

8. Tout traitement de données à caractère personnel doit trouver une base juridique dans l'article 6.1 du RGPD. Les traitements de données instaurés via une mesure normative sont quasiment toujours basés sur l'article 6.1. c) ou e) du RGPD. En vertu de l'article 22 de la *Constitution*, de l'article 8 de la CEDH et de l'article 6.3 du RGPD, de tels traitements doivent être encadrés par une réglementation claire et précise, dont l'application doit être prévisible pour les personnes concernées. La réglementation doit donc définir de manière suffisamment précise sous quelles conditions et dans quelles circonstances le traitement de données à caractère personnel a lieu. En principe, les éléments suivants doivent dès lors y être repris :

a) le responsable du traitement,
b) la (les) finalité(s) du traitement,
c) le type de données nécessaires à la réalisation de cette (ces) finalité(s),

d) la durée de conservation des données,
e) les catégories de personnes concernées dont les données seront traitées,
f) les destinataires ou catégories de destinataires auxquels les données seront communiquées,
g) les circonstances dans lesquelles elles seront communiquées.

C. Traitement de données sensibles

9. L'Autorité attire l'attention sur le fait que le traitement de certaines catégories particulières de données à caractère personnel, telles qu'énumérées aux articles 9 et 10 du RGPD, est en principe interdit.

10. Il s'agit tout d'abord des catégories énumérées à l'article 9.1 du RGPD : les données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que les données génétiques, les données biométriques aux fins d'identifier une personne physique de manière unique, les données concernant la santé et les données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique. L'article 9.2 du RGPD décrit les situations dans lesquelles des exceptions à cette interdiction de traitement s'appliquent. Si de telles catégories de données étaient traitées à la suite d'un projet de texte normatif, il serait donc nécessaire de vérifier si ce traitement trouve une base dans un des motifs d'exception de l'article 9.2 du RGPD.

11. Lors de la préparation d'un projet de texte normatif, l'exception reprise au point g) de l'article 9.2 du RGPD sera souvent pertinente : "*le traitement est nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée*". Si l'auteur d'un projet de texte normatif veut faire reposer (partiellement) un traitement sur cet article 9.2.g) du RGPD, il doit donc démontrer l'intérêt public important qui nécessite le traitement de ces données. En outre, le projet de texte normatif doit prévoir des mesures spécifiques afin de veiller à la protection des droits et intérêts fondamentaux des personnes concernées.

12. L'Autorité fait par ailleurs remarquer que l'article 9 de la LTD impose des conditions complémentaires pour le traitement de ces catégories de données.

13. Une deuxième catégorie de données à laquelle une interdiction de traitement s'applique concerne les données relatives aux condamnations pénales et aux infractions (article 10 du RGPD). Le traitement de ce type de données ne peut être effectué que sous le contrôle de l'autorité publique

ou d'une autre personne si le traitement est autorisé par une loi (nationale ou européenne). Tout registre complet des condamnations pénales ne peut être tenu que sous le contrôle de l'autorité publique. Enfin, l'article 10 de la LTD définit les personnes/organismes qui peuvent traiter ce type de données et sous quelles conditions cela doit se faire.

D. Utilisation du numéro de Registre national

14. Si le but est d'instaurer l'utilisation du numéro de Registre national pour des finalités déterminées via un projet de texte normatif, les prescriptions suivantes doivent être respectées.

15. L'article 87 du RGPD dispose que les États membres qui définissent un numéro d'identification national doivent veiller à ce que celui-ci ne soit utilisé que si des garanties appropriées pour les droits et libertés de la personne concernée sont prévues. De telles garanties impliquent que :

- l'utilisation d'un tel numéro soit limitée aux cas dans lesquels cela est strictement nécessaire et proportionnel, étant donné que cette utilisation engendre certains risques ;
- les finalités soient précisées clairement et explicitement afin que l'on puisse entrevoir les types de traitements visés ;
- la durée de conservation et les éventuelles communications à des tiers soient également encadrées ;
- les mesures techniques et organisationnelles encadrent adéquatement son utilisation sécurisée.

16. En outre, l'Autorité attire l'attention sur le fait que le numéro de Registre national ne peut être utilisé que dans la mesure où l' (les) instance(s) en question dispose(nt) de l'autorisation requise, en vertu de la loi du 8 août 1983 *organisant un registre national des personnes physiques* (article 8, § 1er). Conformément à cette disposition, une autorisation d'utilisation du numéro du Registre national n'est pas requise lorsque cette utilisation est explicitement prévue par ou en vertu d'une loi, un décret ou une ordonnance. Dans les autres cas, l'autorisation d'utiliser le numéro de Registre national est en principe octroyée par le ministre ayant l'Intérieur dans ses attributions, aux conditions énoncées aux articles 5 et 8 de la loi du 8 août 1983. Lorsque le Comité de sécurité de l'information doit émettre une délibération pour une communication de données à caractère personnel, il peut le cas échéant émettre dans le même temps une délibération pour l'utilisation du numéro de Registre national par les instances concernées, si cela s'avère nécessaire dans le cadre de la communication envisagée.

17. Si des données à caractère personnel sont transférées à des pays tiers ou à des organisations internationales, il convient de s'assurer soit que ce transfert ait lieu conformément aux instruments mentionnés aux articles 45 - 48 du RGPD, soit qu'une des situations particulières visées à l'article 49 du RGPD s'applique.

Pour le Centre de Connaissances,
Alexandra Jaspar, Directrice

Autorité de protection des données
Gegevensbeschermingsautoriteit

Advies nr. 136/2021 van 24 augustus 2021

Betreft: Advies m.b.t. een voorstel van resolutie betreffende het bestrijden van cyberfraude via geldezels (CO-A-2021-155)

Het Kenniscentrum van de Gegevensbeschermingsautoriteit (hierna de "Autoriteit"), aanwezig mevrouw Marie-Hélène Descamps, mevrouw Alexandra Jaspar en heren Yves-Alexandre de Montjoye, Bart Preneel en Frank Robben;

Gelet op de wet van 3 december 2017 *tot oprichting van de Gegevensbeschermingsautoriteit,* inzonderheid op artikelen 23 en 26 (hierna "WOG");

Gelet op de Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 *betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG* (hierna "AVG");

Gelet op de wet van 30 juli 2018 *betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens* (hierna "WVG");

Gelet op het verzoek om advies van mevrouw Eliane Tillieux, Voorzitster van de Kamer van Volksvertegenwoordigers, ontvangen op 15/07/2021;

Gelet op het verslag van Alexandra Jaspar;

Brengt op 24 augustus 2021 het volgend advies uit:

I. VOORWERP VAN DE AANVRAAG

1. Mevrouw Eliane Tillieux, Voorzitster van de Kamer van Volksvertegenwoordigers wint het advies van de Autoriteit in m.b.t. een voorstel van resolutie betreffende het bestrijden van cyberfraude via geldezels.

2. In de resolutie wordt gesteld dat cybercriminelen die via het internet mensen geld afhandig maken, veelal "money mules" gebruiken. Om zelf niet betrapt te worden, door bijvoorbeeld het geld rechtstreeks op hun eigen rekening te laten overschrijven, gebruiken de oplichters "geldezels". Deze personen lenen tegen een vergoeding hun bankrekening en/of bankkaart met pincode uit. Het gestolen geld kan zo online uitgegeven worden, naar een andere bankrekening in binnen- of buitenland worden doorgestuurd of aan een bankautomaat worden afgehaald. Vaak is de geldezel de enige die gevat en veroordeeld wordt terwijl de opdrachtgevers buiten schot blijven.

3. Volgens de resolutie is dit het gevolg van het feit dat het de banken aan middelen ontbreekt om het probleem aan de bron te bestrijden. Er is veel meer nood aan uitwisseling van gegevens tussen banken om criminele netwerken te kunnen oprollen naar analogie met het Risk Warning System in Nederland. Dit systeem stelt de banken in staat om onderling onderzoeken te starten bij het witwassen van geld. In de resolutie wordt erop aangedrongen dat de regering een wettelijk kader uitwerkt om het voor de financiële instellingen mogelijk te maken informatie omtrent verdachte rekeningen en transacties uit te wisselen bij een vermoeden van het witwassen van geld, zodat een mogelijk crimineel netwerk makkelijker kan worden opgerold.

II. ONDERZOEK VAN DE AANVRAAG

4. De Autoriteit vestigt er de aandacht op dat het opsporen van criminelen gebeurt door de daartoe gemandateerde overheidsdiensten. Dergelijke onderzoeken gaan immers gepaard met een indringing van de persoonlijke levenssfeer. De vraag stelt zich of het wel de taak is van commerciële ondernemingen zoals banken, die uiteindelijk elkaars concurrenten zijn, om op eigen initiatief onderling onderzoeken op te starten naar hun klanten m.b.t. het witwassen van geld en dus eigenlijk een onderzoek naar strafrechtelijke inbreuken voeren en daarbij gegevens over personen uitwisselen. Dit gaat veel verder dan bijvoorbeeld een meldingsplicht van verdachte transacties aan de bevoegde gerechtelijke autoriteiten die strafonderzoeken voeren met de daarbij horende garanties voor de betrokkenen. Daarenboven leidt het ertoe dat de banken betrokken bij het onderzoek (onderzoeksdoeleinde) in het bezit komen van meer informatie over een klant dan zij in het kader van hun commerciële relatie (commercieel doeleinde) met hem beschikken. Het risico is dan ook aanzienlijk dat de "onderzoeksinformatie" vervolgens commercieel wordt aangewend.

5. Indien overwogen wordt om commerciële ondernemingen een "opsporingsrol" toe te bedelen, dan moet er maximaal naar worden gestreefd om de minimale gegevensverwerking te verzekeren door privacy enhancing technologies. Hierbij kan gedacht worden aan "Private Set Intersection". Daarbij kunnen banken elk een "zwarte lijst" opstellen met mogelijke namen of rekeningen betrokken bij money mules en dan nagaan welke namen ook op de "zwarte lijst" van andere banken voorkomen zonder enige informatie te lekken over gegevens die maar 1 keer voorkomen.

6. Zolang niets precies is uitgewerkt, is het voor de Autoriteit onmogelijk om een standpunt te bepalen. Zij beperkt zich hierna dan ook noodgedwongen tot het in herinnering brengen van de belangrijkste principes die bij de eventuele redactie van regelgeving in acht moeten worden genomen.

A. Noodzakelijkheidstoets

7. Elke verwerking van persoonsgegevens die door regelgeving wordt ingevoerd, houdt in principe een beperking in van het recht op bescherming van persoonsgegevens. Bij de voorbereiding van een ontwerp van normatieve tekst dat verwerkingen van persoonsgegevens omkadert, dient bijgevolg eerst te worden geanalyseerd of de geviseerde maatregel wel noodzakelijk is om het legitiem doel te bereiken dat ermee beoogd wordt. Deze noodzakelijkheidstoets impliceert dat de steller van een ontwerp van normatieve tekst een voorafgaande analyse uitvoert van enerzijds de feiten die de invoering van de maatregel rechtvaardigen en anderzijds de efficiëntiegraad van de maatregel in het licht van het doeleinde dat ermee beoogd wordt. Bij deze analyse dient de steller ook na te gaan of zijn doel eventueel via een maatregel kan bereikt worden die vanuit gegevensbeschermingsoogpunt minder intrusief is.

B. Rechtsgrondslag en voorzienbaarheid van de norm

8. Elke verwerking van persoonsgegevens dient een rechtsgrond te hebben in artikel 6.1 AVG. Gegevensverwerkingen die via een normatieve maatregel worden ingevoerd zijn vrijwel steeds gebaseerd op artikel 6.1. punt c) of e) AVG . Krachtens artikel 22 GW, artikel 8 EVRM en artikel 6.3 AVG, dienen dergelijke verwerkingen omkaderd te worden door duidelijke en nauwkeurige regelgeving, waarvan de toepassing voor de betrokkenen voorzienbaar moet zijn. De regelgeving dient dus op een voldoende precieze manier te bepalen onder welke voorwaarden en in welke omstandigheden de verwerking van persoonsgegevens plaatsvindt. In principe dienen de volgende elementen er daarom in te worden opgenomen:

a) de verwerkingsverantwoordelijke,
b) het (de) doeleinde(n) van de verwerking,

c) het soort gegevens die noodzakelijk zijn voor de verwezenlijking van dit (deze) doeleinde(n),
d) de bewaartermijn van de gegevens,
e) de categorieën betrokkenen van wie de gegevens zullen worden verwerkt,
f) de ontvangers of categorieën ontvangers aan wie de gegevens worden meegedeeld,
g) de omstandigheden waarin ze zullen worden meegedeeld.

C. Verwerking van gevoelige gegevens

9. De Autoriteit wijst er op dat de verwerking van sommige bijzondere categorieën van persoonsgegevens zoals opgesomd in de artikelen 9 & 10 AVG in principe verboden is.

10. Het betreft ten eerste de categorieën opgesomd in artikel 9.1 AVG: de persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, gegevens over gezondheid en gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid. Artikel 9.2 AVG beschrijft de situaties waarin uitzonderingen gelden op dit verwerkingsverbod. Indien dergelijke categorieën van gegevens ingevolge een ontwerp van normatieve tekst verwerkt zullen worden, is het aldus noodzakelijk om na te gaan of deze verwerking een basis vindt in één van de uitzonderingsgronden in artikel 9.2 AVG .

11. Bij de voorbereiding van een ontwerp van normatieve tekst zal vaak de uitzondering onder punt g) van artikel 9.2 AVG relevant zijn: "de verwerking is noodzakelijk om redenen van zwaarwegend algemeen belang, op grond van Unierecht of lidstatelijk recht, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene". Indien de steller van een ontwerp van normatieve tekst een verwerking (ten dele) op dit artikel 9.2.g) AVG wil baseren, dient hij aldus het zwaarwegend algemeen belang aan te tonen dat de verwerking van deze gegevens noodzaakt. Bovendien moet het ontwerp van normatieve tekst specifieke maatregelen treffen om te waken over de bescherming van de grondrechten en de fundamentele belangen van de betrokkenen.

12. De Autoriteit wijst er verder op dat artikel 9 WVG bijkomende voorwaarden oplegt voor de verwerking van deze gegevenscategorieën.

13. Een tweede categorie van gegevens waarvoor een verwerkingsverbod geldt zijn gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten (artikel 10 AVG). Dit soort gegevens mag alleen worden verwerkt onder toezicht van de overheid of een andere persoon indien de

verwerking door een wet (nationaal of Europees) is toegestaan. Omvattende registers van strafrechtelijke veroordelingen mogen alleen worden bijgehouden onder toezicht van de overheid. Tot slot bepaalt artikel 10 WVG door welke personen/instellingen dit type van gegevens kan verwerkt worden en onder welke voorwaarden dit dient te gebeuren.

D. Gebruik van het Rijksregisternummer

14. Indien het de bedoeling is om via een ontwerp van normatieve tekst voor welbepaalde doeleinden het gebruik van het Rijksregisternummer in te voeren, dienen onderstaande voorschriften in acht genomen te worden.

15. Artikel 87 van de AVG stelt dat lidstaten die een nationaal identificatienummer vaststellen er moeten over waken dat dit alleen wordt gebruikt indien er passende waarborgen voor de rechten en vrijheden van de betrokkene worden voorzien. Dergelijke garanties impliceren dat:

- het gebruik van een dergelijk nummer beperkt dient te worden tot de gevallen waarin dit strikt noodzakelijk en proportioneel is, aangezien dit gebruik bepaalde risico's met zich meebrengt;
- de doeleinden duidelijk en expliciet worden gepreciseerd zodat men de beoogde soorten verwerkingen kan vermoeden;
- de bewaartermijn en de eventuele mededelingen aan derden eveneens worden omkaderd;
- de technische en organisatorische maatregelen het beveiligd gebruik passend omkaderen.

16. De Autoriteit vestigt er verder de aandacht op dat het gebruik van het Rijksregisternummer slechts toegestaan is voor zover de betrokken instantie(s) over de vereiste machtiging beschik(t)(ken), op grond van de wet van 8 augustus 1983 *tot regeling van een Rijksregister van de natuurlijke personen* (artikel 8, § 1) . Overeenkomstig deze bepaling is er geen machtiging vereist om het Rijksregisternummer te gebruiken wanneer dit gebruik uitdrukkelijk voorzien is door of krachtens een wet, een decreet of een ordonnantie. In de andere gevallen wordt de machtiging tot gebruik van het Rijksregisternummer in principe verleend door de minister bevoegd voor Binnenlandse Zaken, onder de voorwaarden bepaald in de artikelen 5 en 8 van de wet van 8 augustus 1983. Wanneer het Informatieveiligheidscomité een beraadslaging moet verlenen voor een mededeling van persoonsgegevens kan hij in voorkomend geval tegelijk een beraadslaging verlenen voor het gebruik van het Rijksregisternummer door de betrokken instanties, indien dat noodzakelijk is in het kader van de beoogde mededeling.

17. Indien persoonsgegevens worden doorgegeven aan derde landen of een internationale organisatie moet erover gewaakt worden dat dit gebeurt hetzij overeenkomstig de instrumenten vermeld in de artikelen 45 - 48 AVG dan wel dat een van de specifieke situaties vermeld in artikel 49 AVG van toepassing is.

Voor het Kenniscentrum,
Alexandra Jaspar, Directeur