



## Advies 123/2018 van 7 november 2018

**Betreft:** Adviesaanvraag betreffende een ontwerp van Koninklijk besluit waarbij de informatieplichtigen jegens het centraal aanspreekpunt van rekeningen en financiële contacten gemachtigd worden tijdelijk toegang te hebben tot het Rijksregister van de natuurlijke personen (CO-A-2018-106)

De Gegevensbeschermingsautoriteit (hierna "de Autoriteit");

Gelet op de wet *van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit*, inzonderheid op artikel 23 en 26;

Gelet op het verzoek om advies van de heer Johan Van Overtveldt, Minister van Financiën, ontvangen op 14 september 2018;

Gelet op het verslag van de heer Willem Debeuckelaere;

Brengt op 7 november 2018 het volgend advies uit:

## **I. ONDERWERP EN CONTEXT VAN DE ADVIESAANVRAAG**

1. Op 14 september laatstleden ontving de Autoriteit een adviesaanvraag van de heer Johan Van Overtveldt, Minister van Financiën betreffende het ontwerp van Koninklijk besluit waarbij de informatieplichtigen jegens het centraal aanspreekpunt van rekeningen en financiële contacten gemachtigd worden tijdelijk toegang te hebben tot het Rijksregister van de natuurlijke personen.
2. De wet 8 juli 2018 houdende organisatie van dit centraal aanspreekpunt bij de Nationale Bank van België verplicht de instellingen en professionals bedoeld in artikel 3 van deze wet om de financiële informatie, beschreven in artikel 4 van diezelfde wet (rekeningnummer, identiteit van de klant en in voorkomend geval van zijn volmachtouder, bestaan van financiële verrichtingen waarbij contanten betrokken zijn, bestaan van kredietopeningen, leningen of leasingovereenkomsten,...) van hun klanten aan dit aanspreekpunt mee te delen. Het is dat deze gegevens zouden beschikbaar zijn in het raam van een fiscaal onderzoek, de opsporing van strafbare feiten en de strijd tegen witwaspraktijken en tegen de financiering van terrorisme en groot banditisme of nog het opmaken van een erfenisaangifte door een notaris.
3. Artikel 12 van deze wet machtigt de informatieplichtigen van het verstrekken van financiële informatie om het Rijksregisternummer te gebruiken in het raam van hun verplichte gegevensmededelingen aan het centraal aanspreekpunt. Deze wettelijke bepaling voorziet dat deze instellingen en personen beschikken over een onrechtstreekse toegang tot het Rijksregister teneinde er het Rijksregisternummer van een klant of een volmachtouder op te zoeken en dit gedurende 13 of maximum 19 maanden, te rekenen vanaf de publicatie van deze wet in het Belgisch Staatsblad. Artikel 12, §1, 2<sup>de</sup> lid verleent aan de Koning de bevoegdheid om de werkingsvoorwaarden vast te leggen van de tussenkomende instelling die zal instaan voor de opzoekingen in het Rijksregister voor rekening van de informatieplichtigen. Het is deze bepaling die voorliggend ontwerp van koninklijk besluit wenst uit te voeren.

## **II. ONDERZOEK TEN GRONDE**

4. Het ontwerp van koninklijk besluit bepaalt sommige voorwaarden waaraan de instellingen bedoeld in voormeld artikel 12 moeten voldoen om gemachtigd te worden om toegang te krijgen tot het Rijksregister. Het duidt de aangewezen instelling nominatief aan en preciseert de modaliteiten en beperkingen waarbinnen deze het Rijksregister zal kunnen raadplegen voor rekening van de informatieplichtigen.

5. Zodoende overschrijdt de Koning zijn bevoegdheden aangezien het Sectoraal comité van het Rijksregister bevoegd is voor het afleveren van machtigingen voor toegang tot het Rijksregister krachtens artikel 5 van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen (hierna WRR) en artikel 114, §4 van de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit<sup>1</sup>. Enkel een in de Ministerraad overlegd Koninklijk besluit kan de gevallen bepalen waarin geen voorafgaande machtiging van het Sectoraal comité van het Rijksregister is vereist (art. 5 in fine WRR).
  
6. Bovendien zijn vele bepalingen van het ontwerp van koninklijk besluit overtollig ten opzichte van wat reeds is bepaald hetzij in de WRR, hetzij door artikel 12 van de voormelde wet van 8 juli 2018 en kunnen derhalve worden geschrapt. Het gaat om de artikel 1, 1° en 3° van het ontwerp (verwijzing naar artikel 5 van de WRR tot vaststelling van de ontvankelijkheidsvoorwaarden van de aanvragen voor toegang tot het Rijksregister, noodzaak van het bestaan van een mandaat tussen Identifin en de informatieplichtige zoals reeds voorzien in artikel 12 van de voormelde wet van 8 juli 2018), om artikel 2, 1° van het ontwerp (lijst van de gegevens van het Rijksregister die kunnen geraadpleegd worden voor dit doeleinde - reeds vastgesteld door artikel 12 van de voormelde wet en vaststelling van het doeleinde waarvoor het Rijksregisternummer mag worden gebruikt - reeds voorzien door artikel 12 van de voormelde wet) en ten slotte, om punt a) van artikel 2, 2° van het ontwerp (tijdelijke beperking van de toegang tot het Rijksregister, ook reeds voorzien door dit artikel 12).
  
7. Artikel 2, 2° b) van het ontwerp van Koninklijk besluit stelt dat Identifin geen enkele opzoeking in het Rijksregister mag verrichten indien deze vereniging nog niet in het bezit is van de door de informatieplichtige ingevulde informatieveiligheidsformulieren of ze de garantie niet heeft dat de consulent inzake informatieveiligheid en de informatieveiligheidsvoorzieningen van de informatieplichtige voorafgaandelijk door het Sectoraal comité van het Rijksregister werden goedgekeurd. Welnu, het Sectoraal comité van het Rijksregister beschikt niet over een dergelijke bevoegdheid. Volgens de recente rechtspraak van dit Comité legt dit laatste in zijn beraadslagingen de voorwaarden vast waaraan de door de gemachtigden aangestelde informatieveiligheidsconsulenten moeten voldoen<sup>2</sup>. In de plaats van te verwijzen naar deze

---

<sup>1</sup> De Gegevensbeschermingsautoriteit vestigt eveneens de aandacht op de toepassing van de wet tot oprichting van het informatieveiligheidscomité en tot wijziging van diverse wetten betreffende de uitvoering van verordening (EU) 2016/679 van 27 april 2016 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van richtlijn 95/46/EG

<sup>2</sup> Deze werden in het algemeen als volgt uitgevaardigd: "De gemachtigde wijst een consulent aan op grond van zijn professionele kwaliteiten en deskundigheid, in het bijzonder op het gebied van de praktijk inzake gegevensbescherming en de in de context relevante regelgeving. Deze capaciteiten stellen de consulent in staat diens taken te vervullen en een gedegen kennis te verwerven van de informatica-omgeving van de gemachtigde en van de informatiebeveiliging. De consulent dient deze kennis permanent op peil te houden.

De consulent brengt rechtstreeks verslag uit aan de hoogste leidinggevende van de machtigingsgerechtigde.

voorafgaande goedkeuring, is het aangewezen in de wettelijke bepalingen de vereiste voorwaarden te preciseren, hetzij wat betreft de hoedanigheid van de veiligheidsconsulent als ook wat betreft de veiligheidsmaatregelen die elke informatieplichtige zou moeten goedkeuren.

8. Bovendien, betreffende diezelfde bepaling van het ontwerp stelt de Autoriteit zich vragen bij het niet-cumulatief karakter van de vooraf door de informatieplichtigen te vervullen voorwaarden opdat Identifin voor hun rekening een opzoeking in het Rijksregister zou kunnen uitvoeren. Het optionele karakter van deze voorwaarden lijkt niet gerechtvaardigd en strijdig met andere wettelijke bepalingen. Immers, zowel de veiligheid als het feit dat een fonetische opzoeking in het Rijksregister op basis van een minimaal aantal criteria uit te voeren kan niet optioneel zijn aangezien deze voortvloeien uit reeds bestaande wettelijke vereisten van een hogere rangorde, hetzij krachtens de WRR (art. 10 en 11 WRR)<sup>3</sup> of krachtens artikel 12 van de voormelde wet van 8 juli 2018 (art.12, § 1, 3<sup>de</sup> lid).

---

Ongeacht of de consulent een personeelslid is of iemand extern, mag er geen sprake zijn van een belangenconflict tussen de functie als consulent en andere activiteiten die hiermee onverenigbaar zijn. In het bijzonder kan de functie niet gecumuleerd worden met deze van leidinggevende bestuurder van de informaticadienst of van hoogste leidinggevende van de gemachtigde (bv. algemeen directeur).

De gemachtigde waakt erover dat de consulent zijn opdracht volledig onafhankelijk kan uitoefenen en dat hij geen instructies ontvangt met betrekking tot de uitvoering van die taken. De consulent wordt door de gemachtigde niet ontslagen of gestraft voor de uitvoering van zijn taken.

Indien de taken van consulent aan meerdere personen wordt toevertrouwd, dient aan één van hen de eindverantwoordelijkheid gegeven te worden om te rapporteren over de gezamenlijke werkzaamheden aan de hoogste leidinggevende en om de rol van contactpersoon ten aanzien van het Comité op te nemen.

De gemachtigde ondersteunt de consulent door hem de middelen en tijd te geven die nodig zijn om zijn taken te vervullen en zijn deskundigheid op peil te houden. Met name wordt de consulent de nodige toegang verschaft tot persoonsgegevens en verwerkingsactiviteiten. De gemachtigde zorgt ervoor dat de consulent naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. (cf. bijvoorbeeld in die zin Beraadslaging RR 06/2018)

<sup>3</sup> Enkel het vereisen van een door de Informatieplichtige ingevuld informatiebeveiligingsformulier laat niet toe een beeld te vormen over de kwaliteit van de genomen beveiligingsmaatregelen. Het ware eerder aangewezen minimaal te nemen beveiligingsmaatregelen uit te vaardigen. Hiertoe zou de wetgever zich kunnen laten inspireren door de formulieren die reeds gebruikt werden door het Sectoraal comité van het Rijksregister: (1) De risico's die de verwerkte persoonsgegevens lopen, evalueren en de daarmee verbonden beveiligingsbehoeften vaststellen, (2) Een geschreven document – het beveiligingsbeleid – opstellen waarin de strategieën en de weerhouden maatregelen voor gegevensbeveiliging worden omschreven, (3) Alle mogelijke dragers die de verwerkte persoonsgegevens bevatten, identificeren, (4) De interne en externe personeelsleden die bij de verwerking van persoonsgegevens betrokken zijn, ten aanzien van de verwerkte gegevens inlichten over de vertrouwelijkheids- en beveiligingsverplichtingen die zowel voortvloeien uit de verschillende wettelijke vereisten als uit het beveiligingsbeleid, (5) passende beveiligingsmaatregelen nemen om een niet-gemachtigde of onnodige fysieke toegang te verhinderen tot de dragers die verwerkte persoonsgegevens bevatten, (6) De noodzakelijke maatregelen nemen om elke fysieke schade die de verwerkte persoonsgegevens in gevaar zouden kunnen brengen, te verhinderen, (7) De verschillende netwerken gekoppeld aan de apparatuur die de persoonsgegevens verwerkt, beschermen, (8) een actuele lijst opmaken van de verschillende bevoegde personen die in het kader van de verwerking toegang hebben tot de persoonsgegevens alsook van hun respectieve toegangsniveau (creatie, raadpleging, wijziging, vernietiging), (9) een mechanisme voor toegangsmachtiging ontwerpen zodat de verwerkte persoonsgegevens en de verwerkingen die betrekking hebben op deze gegevens uitsluitend toegankelijk zijn voor personen en toepassingen die daartoe uitdrukkelijk gemachtigd zijn, (10) een informatiesysteem ontwerpen dat permanente logging, opsporing en analyse mogelijk maakt van de toegang die personen en logische entiteiten gehad hebben tot de verwerkte persoonsgegevens, (11) het voorzien van een controle op de geldigheid en de efficiëntie in de tijd van de geïmplementeerde technische of organisatorische maatregelen, (12) het invoeren van noodprocedures voor het beheren van veiligheidsincidenten met verwerkte persoonsgegevens, (13) het samenstellen en bijwerken van voldoende documentatie met betrekking tot de organisatie van de informatieveiligheid in het raam van de bedoelde verwerking.

9. Artikel 3 van het ontwerp bepaalt dat de vzw Identifin onverwijld de Rijksregisternummers die zij bij het Rijksregister van de natuurlijke personen heeft opgehaald nadat zij deze nummers aan haar volmachtgever heeft meegedeeld zal vernietigen. Een van de voordelen van het voorzien van een tussenpersoon voor het raadplegen van een authentieke bron door de leden van een welbepaalde sector bestaat erin dat deze tussenpersoon beschikt over bevoegdheden inzake controle en verificatie van het conforme karakter van de aanvragen voor toegang met de normen inzake bescherming van persoonsgegevens. De Koning zal de hem krachtens artikel 12 van de voormelde wet van 8 juli 2018 verleende bevoegdheid uitvoeren door auditbevoegdheden toe te kennen aan Identifin. Deze mogen zich niet beperken tot voorafgaande controles maar dienen eveneens mogelijke verificaties a posteriori toe te laten, bijvoorbeeld via punctuele audits bij informatieplichtigen. Hiertoe is de bewaring in de loggings van de Rijksregisternummers van de personen voor wie raadplegingen hebben plaatsgevonden, de identificatie van de informatieplichtigen en hun aangestelden die overgegaan zijn tot raadplegingen alsook van het motief van hun raadpleging, onontbeerlijk en dit voor de periode waarin een latere controle opportuun is (in het algemeen 10 jaar na de raadpleging). Artikel 3 zal dus dienovereenkomstig dienen aangepast te worden.

### **OM DIE REDENEN,**

Brengt de Autoriteit een ongunstig advies uit over het voorontwerp van wet wegens niet-eeerbiediging van de bevoegdheden van het Sectoraal comité van het Rijksregister of de voorgeschreven vormen om hiervan af te wijken. Voor het overige stelt de Autoriteit als voorwaarden voor een gunstig advies dat rekening wordt gehouden met volgende voorwaarden:

1. Eerbiediging van de bevoegdheden van het Sectoraal comité van het Rijksregister of van de voorgeschreven vormen om hiervan af te wijken (cons. 5);
2. Schrapping van bepalingen die overbodig zijn in het licht van andere wettelijke bepalingen van een hogere rangorde (cons. 6) ;
3. Vaststelling van de vereiste voorwaarden voor de aan te wijzen veiligheidsconsulent in toepassing van de WRR en van de veiligheidsmaatregelen die de bedoelde gegevensverwerking moeten omkaderen (cons. 7) ;
4. Schrapping van het optionele karakter van voorwaarden die vereist zijn door wettelijke bepalingen van een hogere rangorde (cons. 8) ;

5. Verduidelijking van de controle- en auditbevoegdheden waarover Identifin zal beschikken ten opzichte van de informatieplichtigen en vaststelling van de overeenkomstige bewaartermijn(en) van de raadplegingen (cons. 9)

De Wnd. Administrateur,

De Voorzitter,

(get.) An Machtens

(get.) Willem Debeuckelaere