



Avis n° 123/2018 du 7 novembre 2018

Objet: Avis sur le projet d'Arrêté royal autorisant les redevables d'information au point de contact central des comptes et contrats financiers à accéder temporairement au Registre national des personnes physiques (CO-A-2018-106)

L'Autorité de protection des données (ci-après l'Autorité);

Vu la loi du 3 décembre 2017 *relative à la loi portant création de l'Autorité de protection des données*, en particulier les articles 23 et 26;

Vu la demande d'avis de Monsieur Johan Van Overtveldt, Ministre des finances, reçue le 14 septembre 2018;

Vu le rapport de Monsieur Willem Debeuckelaere;

Émet, le 7 novembre 2018, l'avis suivant :

I. OBJET ET CONTEXTE DE LA DEMANDE D'AVIS

1. L'Autorité a reçu en date du 14 septembre dernier une demande d'avis du Ministre des Finances, Johan Van Overtveldt, sur un projet d'Arrêté royal autorisant les redevables d'information au point de contact central des comptes et contrats financiers à accéder temporairement au Registre national des personnes physiques.
2. La loi du 8 juillet 2018 portant organisation de ce point de contact central établi auprès de la Banque nationale de Belgique oblige les établissements et professionnels visés à l'article 3 de cette loi à communiquer à ce point de contact les informations financières décrites à l'article 4 de cette même loi (numéro de compte, identité du client et le cas échéant de son mandataire, existence de transactions financières impliquant des espèces, existence d'ouverture de crédit, de prêt ou de location-financement, ...) concernant leurs clients. Le but étant que ces informations soient accessibles dans le cadre d'une enquête fiscale, de la recherche d'infractions pénales et de la lutte contre le blanchiment de capitaux et contre le financement du terrorisme et de la grande criminalité ou encore pour l'établissement d'une déclaration de succession par un notaire.
3. L'article 12 de cette loi autorise les titulaires d'une obligation de communication d'informations financières à utiliser le numéro d'identification dans le Registre national dans le cadre de leurs communications obligatoires de données adressées au point de contact central. Cette disposition légale prévoit que ces organismes et personnes disposent d'un droit d'accès indirect au Registre national afin d'y rechercher le numéro d'identification du Registre national d'un client ou mandataire et ce pendant 13 ou maximum 19 mois à dater de la publication de cette loi au Moniteur belge. L'article 12, §1, alinéa 2 confère au Roi le soin de déterminer les conditions de fonctionnement de l'institution intermédiaire qui procédera aux recherches dans le Registre national pour le compte des redevables de l'obligation d'informations financières. C'est cette disposition que le présent projet d'Arrêté royal a pour ambition d'exécuter.

II. EXAMEN QUANT AU FOND

4. Le projet d'Arrêté royal fixe certaines conditions auxquelles les institutions intermédiaires visées à l'article 12 précité doivent répondre pour être autorisées à accéder au Registre national. Il désigne nominativement l'institution désignée et précise les modalités et limites dans lesquelles cette dernière pourra consulter le Registre national pour le compte des redevables d'informations financières.

5. Ce faisant, le Roi outrepassé ses compétences étant donné que c'est le Comité sectoriel du Registre national qui est compétent pour délivrer les autorisations d'accès au Registre national en vertu de l'article 5 de la loi du 8 août 1983 organisant un registre national des personnes physiques (ci-après la « LRN ») et de l'article 114, §4 de la loi du 3 décembre 2017 portant création de l'Autorité de protection des données¹. Seul un Arrêté royal délibéré en Conseil des Ministres peut déterminer les cas dans lesquels une autorisation préalable du Comité sectoriel du Registre national n'est pas requise (art. 5 in fine LRN).

6. De plus, beaucoup de dispositions du projet d'Arrêté royal sont redondantes par rapport à ce qui est déjà prévu soit par la LRN soit par l'article 12 de la loi précitée du 8 juillet 2018 et peuvent à ce titre être supprimées. Il s'agit des articles, 1^{er}, 1^o et 3^o en projet (référence à l'article 5 de la LRN déterminant les conditions de recevabilité des demandes d'autorisation d'accès au Registre national, nécessité de l'existence d'un mandat entre Identifin et le redevable de l'obligation d'information déjà prévue à l'article 12 de la loi précitée du 8 juillet 2018), de l'article 2, 1^o en projet (liste des données du Registre national pouvant être accédées pour cette finalité – déjà déterminée par l'article 12 de la loi précitée et détermination de la finalité pour laquelle le numéro d'identification du Registre national peut être utilisé – déjà prévue par l'article 12 de la loi précitée) et enfin, du point a) de l'article 2, 2^o en projet (limitation temporaire de l'accès au Registre national également déjà prévu par cet article 12).

7. L'article 2, 2^o, b) du projet d'Arrêté royal prévoit qu'aucune recherche dans le Registre national ne pourra être faite par Identifin si cette association n'est pas en possession des formulaires de sécurité de l'information complétés par le redevable d'information ou si elle n'a pas la garantie que le conseiller en sécurité proposé et ses mesures de protection de la sécurité de l'information ont reçu l'approbation préalable du Comité sectoriel du Registre national. Or, le Comité sectoriel du Registre national ne dispose pas d'une telle compétence. Selon la jurisprudence récente de ce Comité, ce dernier édicte dans ses délibérations les conditions auxquelles les conseillers en sécurité désignés par les bénéficiaires des autorisations doivent satisfaire². En lieu et place de se référer à

¹ L'Autorité de protection des données attire également l'attention sur l'application de la loi du 5 septembre 2018 instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en oeuvre du 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.

² Celles-ci étaient généralement édictées en ces termes : « Le bénéficiaire de l'autorisation désigne un conseiller sur la base de ses qualités professionnelles et de ses connaissances spécialisées, en particulier, des pratiques en matière de protection des données et du droit pertinent dans le contexte. Ces capacités permettent au conseiller d'accomplir ses missions et de disposer d'une connaissance suffisante de l'environnement informatique du bénéficiaire de l'autorisation ainsi que de la sécurité de l'information. Le conseiller doit en permanence tenir cette connaissance à jour.

Le conseiller fait directement rapport au niveau le plus élevé de la hiérarchie du bénéficiaire de l'autorisation.

Que le conseiller soit un membre du personnel ou une personne externe, il ne peut pas y avoir de conflit d'intérêts entre la fonction de conseiller et d'autres activités qui sont incompatibles avec cette fonction. En particulier, la fonction ne peut pas être cumulée avec celle de gestionnaire dirigeant du service informatique ni avec celle de personne assumant le niveau le plus élevé de la hiérarchie du bénéficiaire de l'autorisation (par exemple directeur général).

cette approbation préalable, il convient de préciser dans les dispositions légales les exigences requises, que ce soit en terme de qualité du conseiller en sécurité que des mesures de sécurité que tout redevable de l'obligation d'informations financières devrait adopter.

8. En outre, concernant cette même disposition en projet, l'Autorité s'interroge sur le caractère non cumulatif des conditions préalables à remplir dans le chef des redevables d'information pour qu'Identifin puisse lancer, pour leur compte, une recherche dans le Registre national. Le caractère optionnel de ces conditions paraît non justifié et contraire à d'autres dispositions légales. En effet, tant la sécurité que le fait de faire une recherche phonétique dans le Registre national sur base d'un nombre minimal de critères de recherche ne peuvent être optionnel étant donné qu'il résulte d'exigences déjà légalement prévues par des normes de rang supérieur que ce soit en vertu de la LRN (art 10 et 11 LRN)³ ou de l'article 12 de la loi précitée du 8 juillet 2018 (art 12, § 1^{er}, al. 3).
9. L'article 3 en projet prévoit que l'ASBL Identifin détruira sans retard les numéros d'identification de registre national qu'elle a recueillis auprès du registre national, après les avoir communiqués à son mandant. Un des avantages de la mise en place d'un intermédiaire pour la consultation d'une source authentique par des membres d'un secteur déterminé consiste à ce que cet intermédiaire dispose de compétences de contrôle et de vérification du caractère conforme des requêtes d'accès

Le bénéficiaire de l'autorisation veille à ce que le conseiller puisse exercer ses missions en toute indépendance et à ce qu'il ne reçoive aucune instruction pour s'en acquitter. Le conseiller ne peut être relevé de ses fonctions ou pénalisé pour l'exercice de ses missions.

Si les tâches de conseiller sont confiées à plusieurs personnes, la responsabilité finale doit être confiée à une seule d'entre elles pour faire rapport au niveau le plus élevé de la direction quant aux activités communes et pour assumer le rôle de personne de contact à l'égard du Comité.

Le bénéficiaire de l'autorisation fournit au conseiller les ressources et le temps nécessaires pour exercer ses missions et lui permet d'entretenir ses connaissances spécialisées. L'accès aux données à caractère personnel et aux opérations de traitement est notamment fourni au conseiller. Le bénéficiaire de l'autorisation veille à ce que le conseiller soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel ». (cf. par exemple en ce sens la délibération RN 06/2018)

³ Exiger la simple possession de formulaire de sécurité de l'information complété par le redevable d'information ne permet pas d'avoir une vue sur la qualité des mesures de sécurité prises. Il conviendrait plutôt d'édicter les mesures de sécurité minimum à prendre. Pour ce faire, le législateur pourrait s'inspirer des formulaires qui étaient utilisés par le Comité sectoriel du Registre national : (1) La réalisation d'une évaluation des risques encourus par les données à caractère personnel traitées et la définition des besoins de sécurité en conséquence, (2) la tenue d'une version écrite de la politique de sécurité de l'information précisant les stratégies et mesures retenues pour sécuriser les données à caractère personnel traitées, (3) l'identification de tous les supports impliquant des données à caractère personnel traitées, (4) l'information du personnel interne et externe impliqué dans le traitement des données quant à ses devoirs de confidentialité et de sécurité vis-à-vis des données traitées découlant tant des dispositions légales que de la politique de sécurité, (5) l'adoption de mesure de sécurisation physique des données pour prévenir les accès physiques inutiles ou non autorisés aux supports contenant les données à caractère personnel traitées, (6) l'adoption de mesures de sécurité physique et environnementale pour prévenir les dommages physiques pouvant compromettre les données à caractère personnel traitées, (7) l'adoption de mesures de protection des réseaux auxquels sont reliés les équipements traitant les données à caractère personnel, (8) la tenue d'une liste actualisée des différentes personnes habilitées à accéder aux données à caractère personnel dans le cadre du traitement précisant leur niveau d'accès respectif (création, consultation, modification, destruction), (9) la mise en place d'une sécurisation logique des accès aux données via un mécanisme d'autorisation d'accès conçu de façon à ce que les données à caractère personnel traitées et les traitements les concernant ne soient accessibles qu'aux personnes et applications explicitement autorisées, (10) la mise en place d'une journalisation des accès tel que soient réalisés un traçage et une analyse permanente des accès des personnes et entités logiques aux données à caractère personnel, (11) la mise en place d'un contrôle de la validité et de l'efficacité dans le temps des mesures techniques ou organisationnelles implémentées, (12) la mise en place de procédures de gestion d'urgence des incidents de sécurité impliquant les données à caractère personnel traitées, (13) la constitution et tenue à jour d'une documentation suffisante concernant l'organisation de la sécurité de l'information dans le cadre du traitement en question.

aux normes protectrices des données à caractère personnel. Le Roi exécutera utilement la délégation qui lui est accordée en vertu de l'article 12 de la loi précitée du 8 juillet 2018 en conférant des compétences d'audit à Identifin. Celles-ci ne peuvent pas se limiter pas à des vérifications préalables mais doivent également couvrir la possibilité de faire des vérifications a posteriori par le biais par exemple d'audit ponctuel auprès des redevables de l'obligation d'informations financières. Pour ce faire, une conservation dans les loggings des numéros de registre national des personnes à propos desquelles des consultations ont eu lieu, l'identification des redevables d'information et de leurs préposés ayant procédé à ces consultations ainsi que du motif de leur consultation est indispensable et ce pendant la période de contrôle ultérieur opportune (généralement 10 ans après que la réalisation de la consultation). L'article 3 devra être adapté en conséquence.

PAR CES MOTIFS,

l'Autorité émet **un avis défavorable** sur l'avant-projet de loi pour non-respect des compétences du Comité sectoriel du Registre national ou des formes prescrites pour y déroger. Pour le surplus, l'Autorité conditionne le caractère favorable de son avis à la prise en compte des remarques suivantes :

1. Respect des compétences du Comité sectoriel du Registre national ou des formes prescrites pour y déroger (cons. 5);
2. Suppression des dispositions redondantes avec d'autres dispositions légales de rang supérieur (cons. 6) ;
3. Détermination des exigences requises pour le conseiller en sécurité à désigner en application de la LRN et pour les mesures de sécurité devant encadrer le traitement de données visé (cons. 7) ;
4. Suppression du caractère optionnel des exigences requises par des normes légales de rang supérieur (cons. 8) ;
5. Précision des compétences de contrôle et d'audit dont disposera Identifin vis-à-vis des redevables de l'obligation d'informations financières et détermination du ou des délais de conservation des données de consultation en conséquence (cons. 9)

L'Administrateur f.f.,

Le Président

(sé) An Machtens

(sé) Willem Debeuckelaere