

N° 7872⁵

CHAMBRE DES DEPUTES

Session ordinaire 2021-2022

PROJET DE LOI

portant modification de

- 1° la loi modifiée du 19 décembre 2008 ayant pour objet la coopération interadministrative et judiciaire et le renforcement des moyens de l'Administration des contributions directes, de l'Administration de l'enregistrement et des domaines et de l'Administration des douanes et accises et portant modification de
- la loi modifiée du 12 février 1979 concernant la taxe sur la valeur ajoutée;
 - la loi générale des impôts («Abgabenordnung»);
 - la loi modifiée du 17 avril 1964 portant réorganisation de l'Administration des contributions directes;
 - la loi modifiée du 20 mars 1970 portant réorganisation de l'Administration de l'enregistrement et des domaines;
 - la loi modifiée du 27 novembre 1933 concernant le recouvrement des contributions directes et des cotisations d'assurance sociale ;
- 2° la loi modifiée du 27 décembre 1817 sur la perception du droit de succession ;
- 3° la loi modifiée du 7 août 1920 portant majoration des droits d'enregistrement, de timbre, de succession, etc.

* * *

**AVIS DE LA COMMISSION NATIONALE POUR
LA PROTECTION DES DONNEES**

(4.3.2022)

Conformément à l'article 57, paragraphe (1), lettre (c) du règlement n° 2016/679 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 »), auquel se réfère l'article 7 de la loi du 1^{er} août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après désignée la « Commission nationale » ou la « CNPD ») « *conseille, conformément au droit de l'État membre, le parlement national, le gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement* ».

Par courrier en date du 17 août 2021, Monsieur le Ministre des Finances a invité la Commission nationale à se prononcer sur le projet de loi portant modification de 1° la loi modifiée du 19 décembre 2008 ayant pour objet la coopération interadministrative et judiciaire et le renforcement des moyens de l'Administration des contributions directes, de l'Administration de l'enregistrement et des domaines

et de l'Administration des douanes et accises et portant modification de certaines autres lois (ci-après le « projet de loi »).

Selon l'exposé des motifs le projet de loi a pour objet « *d'étendre de manière ciblée, le champ d'application de la loi modifiée du 19 décembre 2008 ayant pour objet la coopération interadministrative et judiciaire et le renforcement des moyens de l'Administration des contributions directes (ci-après « l'ACD »), de l'Administration de l'enregistrement et des domaines (ci-après « l'AED ») et de l'Administration des douanes et accises. En effet, les dispositions proposées instaurent des moyens renforcés, afin de répondre aux besoins de la coopération interadministrative de l'Administration de l'enregistrement, des domaines et de la TVA. Les besoins en matière de contrôle de la TVA, de la taxe d'abonnement et de gestion efficace du domaine de l'Etat, vont, en effet, au-delà des dispositions actuellement en vigueur* ».

Il est encore précisé qu'« *[a]fin que l'AED puisse au mieux remplir ses missions légales, à savoir l'établissement correct des différents impôts et des taxes, la lutte contre la fraude fiscale et la garantie du principe de l'égalité des citoyens et des entreprises devant l'impôt, il s'avère en effet nécessaire de compléter et d'élargir le champ d'application de l'échange d'informations avec les acteurs étatiques concernés. Ainsi, le projet de loi consacre le principe d'une coopération étroite et crée le cadre légal concernant l'échange d'informations entre l'AED et le Centre commun de la sécurité sociale (CCSS), le ministre ayant les Transports dans ses attributions, le ministre ayant les autorisations d'établissement dans ses attributions, la Commission de surveillance du secteur financier (CSSF) et l'Agence pour le développement de l'emploi (ADEM). En effet, ces institutions détiennent des informations nécessaires à l'établissement correct et au recouvrement des différents impôts et des taxes relevant des attributions de l'AED* ».

Le présent avis limitera ses observations aux questions traitant des aspects portant sur la protection des données.

1. Remarques liminaires

Conformément à l'article 5, paragraphe (1), lettre b), du RGPD les données personnelles doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités.

Le considérant 50 du RGPD énonce que « *[l]e traitement de données à caractère personnel pour d'autres finalités que celles pour lesquelles les données à caractère personnel ont été collectées initialement ne devrait être autorisé que s'il est compatible avec les finalités pour lesquelles les données à caractère personnel ont été collectées initialement. Dans ce cas, aucune base juridique distincte de celle qui a permis la collecte des données à caractère personnel n'est requise. Si le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement, le droit de l'Union ou le droit d'un État membre peut déterminer et préciser les missions et les finalités pour lesquelles le traitement ultérieur devrait être considéré comme compatible et licite. (...) La base juridique prévue par le droit de l'Union ou le droit d'un État membre en ce qui concerne le traitement de données à caractère personnel peut également constituer la base juridique pour un traitement ultérieur. Afin d'établir si les finalités d'un traitement ultérieur sont compatibles avec celles pour lesquelles les données à caractère personnel ont été collectées initialement, le responsable du traitement, après avoir respecté toutes les exigences liées à la licéité du traitement initial, devrait tenir compte, entre autres: de tout lien entre ces finalités et les finalités du traitement ultérieur prévu; du contexte dans lequel les données à caractère personnel ont été collectées, en particulier les attentes raisonnables des personnes concernées, en fonction de leur relation avec le responsable du traitement, quant à l'utilisation ultérieure desdites données; la nature des données à caractère personnel; les conséquences pour les personnes concernées du traitement ultérieur prévu; et l'existence de garanties appropriées à la fois dans le cadre du traitement initial et du traitement ultérieur prévu.* ».

En ce qui concerne les conditions à respecter dans le cadre d'un traitement à une fin autre que celle pour laquelle les données ont été collectées, celles-ci sont fixées par l'article 6, paragraphe (4), du RGPD, qui dispose que « *[l]orsque le traitement à une fin autre que celle pour laquelle les données ont été collectées n'est pas fondé sur le consentement de la personne concernée ou sur le droit de l'Union ou le droit d'un État membre qui constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir les objectifs visés à l'article 23, paragraphe 1, le responsable du*

traitement, afin de déterminer si le traitement à une autre fin est compatible avec la finalité pour laquelle les données à caractère personnel ont été initialement collectées, tient compte, entre autres :

- a. de l'existence éventuelle d'un lien entre les finalités pour lesquelles les données à caractère personnel ont été collectées et les finalités du traitement ultérieur envisagé ;
- b. du contexte dans lequel les données à caractère personnel ont été collectées, en particulier en ce qui concerne la relation entre les personnes concernées et le responsable du traitement ;
- c. de la nature des données à caractère personnel, en particulier si le traitement porte sur des catégories particulières de données à caractère personnel, en vertu de l'article 9, ou si des données à caractère personnel relatives à des condamnations pénales et à des infractions sont traitées, en vertu de l'article 10 ;
- d. des conséquences possibles du traitement ultérieur envisagé pour les personnes concernées ;
- e. de l'existence de garanties appropriées, qui peuvent comprendre le chiffrement ou la pseudonymisation ».

Comme rappelé à juste titre par le Conseil d'Etat dans son avis du 1^{er} février 2022 relatif au projet de loi¹ « (...) dans la mesure où, dans le cadre du projet sous avis, des données à caractère personnel seront transférées à une autorité publique autre que le responsable du traitement initial pour une finalité différente de celle pour laquelle ces données ont été collectées, cette autorité devra vérifier les conditions alternatives de l'article 6, paragraphe 4, du RGPD qui permettent le traitement ultérieur des données². Le transfert des données entre autorités publiques peut être légitime si le traitement ultérieur est fondé sur une disposition légale qui constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir un des objectifs visés à l'article 23, paragraphe 1, du RGPD ».

En outre, « [d]ans le respect de l'article 11, paragraphe 3, de la Constitution, qui érige en matière réservée à la loi les exceptions à la garantie par l'Etat de la protection de la vie privée, les conditions dans lesquelles les données peuvent être traitées à une finalité autre que celle pour laquelle elles ont été collectées doivent faire l'objet d'une loi, du moins quant aux éléments essentiels de la matière »³.

Par ailleurs, et comme relevé par le Conseil d'Etat dans son avis précité du 1^{er} février 2022, la finalité poursuivie par les acteurs étatiques concernés par le projet de loi, serait susceptible de constituer « une mesure nécessaire et proportionnée dans une société démocratique pour garantir les objectifs visés à l'article 23, paragraphe 1, du RGPD ». En effet, comme rappelé par le Conseil d'Etat dans cet avis « la Cour de Justice de l'Union européenne a reconnu que « contribuer à la lutte contre la fraude et l'évasion fiscale internationales [...] constitue un objectif d'intérêt général par l'Union »⁴.

Ainsi, s'il y a lieu de féliciter les auteurs du projet de loi d'avoir précisé les dispositions légales visant à encadrer « l'échange d'informations avec les acteurs étatiques concernés » par le projet de loi, il convient néanmoins de relever que certaines précisions mériteraient d'être apportées.

La Commission nationale détaillera ces points dans ses développements ci-après.

2. Sur l'article 1 du projet de loi

L'article 1 du projet de loi a pour objet de remplacer l'article 10 de la loi modifiée du 19 décembre 2008 ayant pour objet la coopération interadministrative et judiciaire et le renforcement des moyens de l'ACD, de l'AED et de l'Administration des douanes et accises (ci-après la « loi modifiée du 19 décembre 2008 »).

1 Document parlementaire n°7872/04 du 1^{er} février 2022

2 Cf. Avis du Conseil d'Etat n° 53.126 du 11 juin 2019 sur le projet de loi concernant la limitation de la portée de certains droits et obligations dans le cadre du règlement général sur la protection des données et portant : 1. exécution, en matière de surveillance du secteur financier et des assurances, 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 (règlement général sur la protection des données) ; 2. modification de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier ; et 3. modification de la loi modifiée du 7 décembre 2015 sur le secteur des assurances (doc. parl. n° 73733, p. 4) ; Avis n°60.001 du 27 avril 2021 sur le projet de loi relative à la concurrence (doc. parl. n° 74798, p. 14).

3 En ce sens, voir M. Besch, « Traitement de données à caractère personnel dans le secteur public », Normes et légistique en droit public luxembourgeois, Luxembourg, Promoculture Larcier, 2019, p.472, n°619.

4 CJUE, C-245/19 et C-246/19, *Etat luxembourgeois*, 6 octobre 2020, §86-87

Les dispositions de l'article 10, tel que remplacé par le projet de loi, prévoient une transmission du relevé des travailleurs indépendants affiliés par le CCSS par voie informatique à l'ACD et à l'AED « *en vue de l'établissement correct des impôts directs et de la [TVA] à des revenus et chiffres d'affaires provenant de l'exercice d'une profession agricole, libérale, artisanale ou commerciale* ».

Les auteurs du projet de loi justifient une telle communication car les moyens actuels de l'ACD et de l'AED ne sont pas « *suffisants pour identifier tous les travailleurs indépendants qui exercent une activité au Luxembourg* ».

L'article précise que les données communiquées par le CCSS à l'ACD et à l'AED seraient « *le relevé des travailleurs indépendants affiliés avec leurs nom, prénom, adresse, matricule, genre et lieu de l'activité* ».

Il y a lieu de féliciter les auteurs du projet de loi d'avoir précisé quelles seraient les données à caractère personnel qui seraient communiquées ainsi que les finalités pour lesquelles elles seraient transmises.

En ce qui concerne la communication du numéro d'identification national, la Commission nationale comprend que celui-ci serait communiqué sur base de l'article 2, paragraphe (2) de la loi du 19 juin 2013 relative à l'identification des personnes physiques.

3. Sur l'article 2 du projet de loi

L'article 2 du projet de loi a pour objet d'introduire un nouvel article 10bis dans la loi modifiée du 19 décembre 2018 dont les dispositions visent à instaurer la base légale pour la communication par le CCSS par voie électronique à l'AED du « *nombre total de salariés employés par entreprise ainsi que la masse salariale totale par entreprise sur base annuelle* » en vue de la vérification de l'exacte perception de la TVA.

Selon le commentaire des articles aucune donnée à caractère personnel ne serait communiquée. Dès lors, dans une telle hypothèse le RGPD n'aurait pas vocation à s'appliquer.

4. Sur l'article 3 du projet de loi

L'article 3 du projet de loi a pour objet d'introduire un nouveau paragraphe (2) à l'article 14 de la loi modifiée du 19 décembre 2018.

Cet article dispose qu' « *[e]n vue de la vérification de l'exacte perception de la taxe sur la valeur ajoutée, le ministère ayant les Transports dans ses attributions transmet par voie électronique à l'Administration de l'enregistrement, des domaines et de la TVA les données suivantes relatives aux véhicules soumis à l'immatriculation et détenus par des assujettis à la TVA :*

1. *Le nom du titulaire du certificat d'immatriculation du véhicule ou le cas échéant les noms des propriétaires ou détenteurs du véhicule pour autant que ceux-ci sont enregistrés dans la base de données nationale des véhicules automoteurs ainsi que leur numéro de matricule national ;*
2. *Le numéro de châssis, le numéro d'immatriculation, la marque et le modèle du véhicule, la catégorie de véhicule, la forme de carrosserie, les dates des mises en circulation et hors circulation, la date de la 1ère mise en circulation, la date de mise en circulation au Grand-Duché de Luxembourg, ainsi que les franchises de la taxe sur la valeur ajoutée en matière de véhicules.*

Les conditions, critères et modalités de l'échange entre le ministère ayant les Transports dans ses attributions et l'Administration de l'enregistrement des domaines et de la TVA sont déterminés par règlement grand-ducal. ».

Il y a lieu de féliciter les auteurs du projet de loi d'avoir précisé quelles seraient les données à caractère personnel qui seraient transmises en vue de la vérification de l'exacte perception de la TVA, par le ministre ayant les Transports dans ses attributions à l'AED.

Cependant, il y a lieu de regretter que le projet de règlement grand-ducal ayant pour objet de fixer les conditions, critères et modalités de l'échange n'ait pas été transmis à la CNPD en même temps que le projet de loi afin d'apprécier si celui-ci soulèverait des problématiques d'un point de vue de la protection des données.

5. Sur l'article 4 du projet de loi

L'article 4 du projet de loi a pour objet d'introduire 4 nouveaux articles à la suite de l'article 15 de la loi modifiée du 19 décembre 2008 précitée à savoir les nouveaux articles 15bis (A), 15ter (B), 15quater (C) et 15quinquies (D).

A. Sur l'article 15bis

L'article 15bis a pour objet de prévoir un accès direct à l'AED « *par un système informatique, au registre des entreprises du ministre ayant les autorisations d'établissement dans ses attributions* » en vue de la vérification de l'exacte perception de la TVA.

D'après l'avis du Conseil d'Etat précité, il s'agirait de l'accès au registre des autorisations d'établissement « *qui, par ailleurs, est déjà accessible au public via le site Guichet.lu* ».

Dans la mesure où la terminologie employée par le Conseil d'Etat diffère de celle employée par les auteurs du projet de loi, il y a lieu de s'interroger sur le registre qui serait effectivement visé par le texte sous avis.

La Commission nationale se demande s'il ne s'agirait pas du registre des entreprises visé à l'article 32, paragraphe (1) de la loi modifiée du 2 septembre 2011 réglementant l'accès aux professions d'artisan, de commerçant, d'industriel ainsi qu'à certaines professions libérales?

En tout état de cause, il y a lieu de regretter que les modalités d'accès à un tel registre ne soient pas précisées par les auteurs du projet de loi.

Enfin, il convient de rappeler qu'en vertu du principe de minimisation des données, seules les données à caractère personnel qui sont nécessaires à la réalisation des finalités poursuivies par le responsable du traitement, à savoir la vérification de l'exacte perception de la TVA, devraient être consultées.

B. Sur l'article 15 ter

L'article 15ter a pour objet de prévoir la communication par l'ADEM à l'AED des « *informations et pièces relatives aux abus constatés en matière de travail clandestin réalisé par des bénéficiaires de prestations chômage* »⁵ et la communication par l'AED à l'ADEM « *des infractions constatées en matière de TVA par des bénéficiaires de prestations de chômage* »⁶.

Les auteurs du projet de loi précisent dans le commentaire des articles qu'il « *est créé entre les deux administrations un échange d'informations bidirectionnel ciblé* » et que « *la présente disposition introduit la possibilité d'un échange d'informations limité entre services compétents, permettant d'agir plus efficacement contre ces distorsions de concurrence par rapport aux secteurs économiques concernés et de sécuriser les intérêts du Trésor en matière de TVA à percevoir, d'une part, et de prestations de chômage à rembourser, d'autre part* ».

En outre, ils précisent également que le ministre du Travail et l'ADEM ont d'ores et déjà un accès direct « *aux bases de données relatives à la TVA* » tel que cela est prévu à l'article L.621-3 du Code du travail « *sans réciprocité toutefois* ».

S'il y a lieu de féliciter les auteurs du projet de loi d'avoir prévu le principe d'un tel échange de données à caractère personnel, il y a lieu de regretter, à l'instar du Conseil d'Etat, que les dispositions sous avis ne précisent pas quelles seraient les finalités pour lesquelles les données seraient communiquées, ni quelles seraient les catégories de données visées.

En effet, en ce qui concerne les catégories de données qui feraient l'objet d'un tel échange, le projet de loi indique qu'il s'agirait des « *informations et pièces relatives aux abus constatés en matière de travail clandestin* » et des « *infractions constatées en matière de TVA par des bénéficiaires de prestations de chômage* ».

Or, en l'absence de précisions à ce sujet dans le commentaire des articles, et dans la mesure où ces dispositions sont formulées de manière trop vague, il y a lieu de s'interroger sur les catégories de données qui seraient effectivement visées par de telles dispositions.

En outre, il y a lieu de relever que si les finalités d'un tel échange de données sont précisées dans le commentaire des articles, celles-ci ne figurent pas dans le texte du projet de loi.

Or, il convient de rappeler qu'afin de respecter les exigences de clarté, de précision et de prévisibilité auxquelles un texte légal doit répondre, et conformément à la jurisprudence de la Cour de justice de

⁵ Article 15ter paragraphe (1) du projet de loi

⁶ Article 15ter paragraphe (2) du projet de loi

l'Union européenne et de la Cour européenne des droits de l'homme⁷, les auteurs du projet de loi devraient apporter de telles précisions dans le texte sous avis.

En l'absence de telles précisions, la Commission nationale n'est, dès lors, pas en mesure d'apprécier si le principe de minimisation des données serait respecté en l'espèce.

C. Sur l'article 15quater

L'article 15quater a pour objet de prévoir que la CSSF fournit sur demande de l'AED « *tous renseignements, actes et documents en sa possession et concernant les entités soumises à sa surveillance, dès lors que ces renseignements, actes et documents sont nécessaires à l'[AED] dans le cadre de l'exercice strict de sa mission légale pour la vérification de l'exacte perception de la taxe sur la valeur ajoutée et de la taxe d'abonnement* ».

Les dispositions prévoient encore que les informations obtenues ne peuvent être utilisées qu'aux fins pour lesquelles elles ont été communiquées.

Enfin, l'article sous avis précise encore que lorsque les informations proviennent d'autorités étrangères, leur transmission par la CSSF à l'AED ne peut se faire qu'avec l'accord explicite desdites autorités.

S'il y a lieu de féliciter les auteurs du projet de loi pour de telles précisions, la CNPD tient à formuler les observations ci-après.

En ce qui concerne l'échange d'informations en vue de la vérification de l'exacte perception de la TVA, il ressort du commentaire des articles que les renseignements, actes et documents qui seraient transmis à l'AED seraient ceux visés par « *les dispositions du règlement grand-ducal du 14 décembre 2011 déterminant la procédure de dépôt de la liasse comptable, de l'article 8 du Code de commerce et de l'article 75 de la loi modifiée du 19 décembre 2002 concernant le registre de commerce et des sociétés ainsi que la comptabilité et les comptes annuels des entreprises, les entités soumises à la surveillance de la CSSF (à l'exception des PSF de support) qui sont dispensées d'établir et de déposer leurs bilans, comptes de résultat et leur plan comptable sur la base eCDF, c'est-à-dire de manière standardisée* ».

Il y a lieu de rappeler que le RGPD n'aura vocation à s'appliquer que si l'échange tel qu'il est prévu par le projet de loi implique un traitement de données à caractère personnel.

A ce titre, il convient de préciser que l'article 4 du RGPD définit comme données à caractère personnel « *toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée ») ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* ».

De plus, le considérant 14 du RGPD dispose que « *[l]e présent règlement ne couvre pas le traitement des données à caractère personnel qui concernent les personnes morales, et en particulier des entreprises dotées de la personnalité juridique, y compris le nom, la forme juridique et les coordonnées de la personne morale* ». Cependant, des informations ayant trait à des personnes morales peuvent, le cas échéant, concerner des personnes physiques et dès lors être considérées comme des données à caractère personnel.

En effet, le groupe de travail « article 29 »⁸ dans son avis 4/2007 sur le concept de données à caractère personnel du 20 juin 2007, WP 136, indique que « *les informations ayant trait à des personnes morales peuvent également être considérées comme « concernant » des personnes physiques en tant que telles (...). Cela peut être le cas lorsque le nom de la personne morale est dérivé de celui d'une*

7 En ce sens, voir M. Besch, « Traitement de données à caractère personnel dans le secteur public », Nonnes et légistique en droit public luxembourgeois, Luxembourg, Promoculture Larcier, 2019, p.469, n°619; Voir entre autres CourEDH, Zakharov e. Russie [GCL n°47413/06], § 228-229, 4 décembre 2015, CourEDH, Vavříčka et autres c. République tchèque (requêtes n°47621/13 et 5 autres), § 276 à 293, 8 avril 2021.

8 Le groupe de travail « article 29 » était un organe consultatif qui conseillait la Commission sur les questions de protection des données et qui a contribué à l'élaboration de politiques harmonisées en matière de protection des données dans l'UE. Après l'entrée en application du RGPD le 25 mai 2018, le comité européen de la protection des données a succédé à ce groupe de travail.

personne physique. Un autre cas de figure est celui du courrier électronique d'une entreprise qui est normalement utilisé par un employé, ou des informations concernant une petite entreprise (du point de vue juridique, un « objet » plutôt qu'une personne morale) qui peuvent éventuellement décrire le comportement de leur propriétaire ».

En outre, les « Lignes directrices relatives au règlement concernant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne », COM(2019) 250 final du 29 mai 2019, précisent également dans quel cas des données relatives à des personnes morales sont susceptibles de constituer des données à caractère personnel.

Cependant, dans l'hypothèse où des données à caractère personnel seraient traitées et dans la mesure où le texte sous avis ne précise pas les informations qui seraient communiquées par la CSSF à l'AED, il est difficile d'apprécier si le principe de minimisation des données serait respecté.

Par ailleurs, il y a lieu de féliciter les auteurs du projet de loi d'avoir précisé dans le commentaire des articles que « [l]e dispositif réglementaire concernant la coopération de la CSSF et l'AED s'apprécie comme une exception à l'obligation au secret professionnel de ces deux autorités. Il y a lieu de rappeler que ce secret professionnel est « renforcé », dans la mesure où ses violations sont punies par les sanctions pénales prévues à l'article 458 du Code pénal. Il découle de ce contexte pénal que les exceptions au secret doivent être prévues par une loi et qu'elles sont d'interprétation stricte, et que par conséquent, le cadre permettant l'échange d'information doit être établi par la loi pour établir un niveau adéquat de sécurité juridique. L'AED étant soumise au secret fiscal, les informations qui seront transmises par la CSSF en vertu du présent projet de loi bénéficieront d'une protection au moins équivalente en matière de secret professionnel que celle visée à l'article 16 de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier ».

D. Sur l'article 15quinquies

L'article 15quinquies a pour objet de prévoir que « les ministères, administrations, services et établissements publics de l'Etat, fournissent sur demande à l'[AED] à l'aide de procédés automatisés ou non, tous renseignements, actes et documents en leur possession, qui sont nécessaires pour l'exercice de ses attributions en matière domaniale ».

En l'absence de précisions dans le projet de loi et dans le commentaire des articles sur les renseignements, actes et documents qui seraient, le cas échéant, transmis à l'AED et dans la mesure où les dispositions sont formulées de manière vague, il est difficile d'apprécier si le principe de minimisation des données serait respecté en l'espèce.

A ce titre, il y a lieu de rappeler que seules les données qui seraient nécessaires à l'AED dans le cadre de l'exercice de ses attributions en matière domaniale ne devraient être traitées.

6. Sur le droit à l'information

Il ressort du projet de loi que les données faisant l'objet des échanges visés par le projet de loi, seront collectées de manière indirecte alors qu'elles seront transmises non pas par les personnes concernées directement mais par une administration.

Dès lors, les responsables du traitement devraient, en principe, fournir toutes les informations prévues à l'article 14 du RGPD endéans les délais prévus à l'article 14, paragraphe (3), du RGPD.

Cependant, en vertu de l'article 14, paragraphe (5), du RGPD, l'obligation d'information préalable ne s'applique pas lorsque « l'obtention ou la communication des informations sont expressément prévues par le droit de l'Union ou le droit de l'Etat membre auquel le responsable du traitement est soumis et qui prévoit des mesures appropriées visant à protéger les intérêts légitimes de la personne concernée ».

Ainsi, s'il y a lieu de féliciter les auteurs du projet de prévoir de telles communications dans un texte légal, il convient de constater que le texte sous avis reste muet quant aux mesures appropriées précitées qui seraient, le cas échéant, prévues.

Il conviendrait de s'assurer que de telles mesures soient mises en œuvre et soient aussi prévues dans le projet de texte de loi.

7. Sur la sécurité du traitement

Conformément à l'article 5 paragraphe (1), lettre f), du RGPD les données à caractère personnel doivent être « *traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité)* ».

L'article 32 du RGPD dispose encore que « *le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque* ». Pareilles mesures doivent être mises en œuvre afin d'éviter notamment des accès non-autorisés aux données, des fuites de données ou des modifications non désirées.

Ainsi, dans le cadre de la mise en œuvre d'échanges de données entre les différentes administrations par voie informatique, ou via des procédés automatisés ou non, de telles mesures de sécurité devraient être mises en œuvre par les différents responsables du traitement afin d'assurer la confidentialité et la sécurité des données.

Dans ce contexte, il est vivement recommandé de définir une politique de gestion des accès, afin de pouvoir identifier dès le début la personne ou le service, au sein de chaque administration concernée et à quelles données précises cette personne ou ce service aurait accès.

En outre, il est nécessaire de prévoir un système de journalisation des accès. Sur ce point, la CNPD recommande que les données de journalisation soient conservées pendant un délai de cinq ans à partir de leur enregistrement, délai après lequel elles sont effacées, sauf lorsqu'elles font l'objet d'une procédure de contrôle.

La CNPD souligne aussi l'importance d'effectuer proactivement des contrôles en interne. A cet effet, il convient conformément à l'article 32, paragraphe (1), lettre d) du RGPD de mettre en œuvre une procédure « *visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement* ».

Ainsi décidé à Belvaux en date du 4 mars 2022.

La Commission nationale pour la protection des données

Tine A. LARSEN
Présidente

Thierry LALLEMANG
Commissaire

Alain HERRMANN
Commissaire