

Avis de la Commission nationale pour la protection des données relatif à la loi modifiée du 25 mars 2020 instituant un système électronique central de recherche de données concernant des comptes IBAN et des coffres-forts

Délibération n° 39/AV24/2023 du 9 juin 2023

1. Conformément à l'article 57, paragraphe 1^{er}, 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* ».
2. L'article 36, paragraphe 4 du RGPD dispose que « *[l]es États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement.* »

La Commission nationale a été saisie le 23 décembre 2019 par Monsieur le Ministre des Finances afin de présenter ses réflexions et commentaires relatifs au projet de loi n°7512 instituant un système électronique central de recherche de données concernant des comptes de paiement et des comptes bancaires identifiés par un numéro IBAN et des coffres-forts tenus par des établissements de crédit au Luxembourg et portant 1. transposition a. de l'article 1^{er} points 19 et 29, de la directive (UE) 2018/843 du Parlement européen et du Conseil du 30 mai 2018 modifiant la directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme ainsi que les directives 2009/138/CE et 2013/36/UE ; b. de l'article 1^{er}, point 28, lettre (d), de la directive (UE) 2019/878 du Parlement européen et du Conseil du 20 mai 2019 modifiant la directive 2013/36/UE en ce qui concerne les entités exemptées, les compagnies financières holding, les compagnies financières holding mixtes, la rémunération, les mesures et pouvoirs de surveillance et les mesures de conservation des fonds propres ; c. de l'article 64, point 5, de la directive (UE) 2019/2034 du Parlement européen et du Conseil du 27 novembre 2019 concernant la surveillance prudentielle des entreprises d'investissement et modifiant les directives 2002/87/CE, 2009/65/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE et 2014/65/UE ; et 2. modification: a. de la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme ; b. de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat ; c. de la



loi du 30 mai 2018 relative aux marchés d'instruments financiers ; et d. de la loi du 13 janvier 2019 instituant un Registre des bénéficiaires effectifs (ci-après « le projet de loi »).

3. Le Conseil d'Etat a émis son avis le 10 mars 2020 et formulé quelques observations relatives au projet de loi. Suite à cela, la Commission des Finances et du Budget a, dans son rapport du 19 mars 2020, recommandé à la Chambre des Députés d'adopter le projet de loi tel que modifié suite à l'avis du Conseil d'Etat. Le projet de loi a été adopté en l'état par vote de la Chambre des Députés le 21 mars 2020. Toutefois, « [c]onstatant cependant l'absence de l'avis de la Commission nationale pour la protection des données (ci-après : la CNPD) concernant le projet de loi 7512 », une motion¹ a été concomitamment votée afin d'inviter le Gouvernement :
 - « À prendre part, en temps utile, à la réunion de la Commission des Finances et du Budget qui sera amenée à analyser l'avis de la CNPD sur le projet de loi 7512
 - A évaluer lors de ladite réunion avec les membres de la Commission des Finances et du Budget de l'opportunité d'apporter, sur base de l'avis de la CNPD à venir, des modifications à la loi votée en date de ce jour. »
4. La loi du 25 mars 2020 instituant un système électronique central de recherche de données concernant des comptes de paiement et des comptes bancaires identifiés par un numéro IBAN et des coffres-forts tenus par des établissements de crédit au Luxembourg a été publiée au Mémorial A du Journal Officiel n° 193 du 26 mars 2020 (ci-après « la loi du 25 mars 2020 »).
5. Le 23 juillet 2020, la Circulaire CSSF 20/747 a été publiée afin de préciser les modalités techniques relatives à l'application de la loi du 25 mars 2020². Elle comprend une Annexe 1 précisant les modalités techniques que les professionnels sont appelés à suivre strictement dans la mise en place du système et une Annexe 2 établissant un tableau contenant la description précise de toutes les données devant apparaître dans un fichier.
6. La loi du 25 mars 2020 a depuis été modifiée par :
 - la loi du 25 février 2021 portant modification de : 1° la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme ; 2° la loi modifiée du 20 avril 1977 relative à l'exploitation des jeux de hasard et des paris relatifs aux épreuves sportives ; 3° la loi modifiée du 17 décembre 2010 concernant les organismes de placement collectif ; 4° la loi du 25 mars 2020 instituant un système électronique central de recherche de données concernant des comptes IBAN et des coffres-forts ; 5° la loi du 10 juillet 2020 instituant un Registre des fiducies et des trusts ;
 - la loi du 22 juin 2022 portant sur la gestion et le recouvrement des avoirs saisis ou confisqués ;
 - la loi du 28 octobre 2022 portant création de la procédure de dissolution administrative sans liquidation ; et

¹ https://www.chd.lu/fr/motion_resolution/3156

² <https://www.cssf.lu/fr/document/circulaire-cssf-20-747/>



- la loi du 16 mai 2023 relative à l'échange automatique et obligatoire des informations déclarées par les Opérateurs de Plateforme.
7. Au vu de ce qui précède, le présent avis de la CNPD portera sur la loi modifiée du 25 mars 2020 (ci-après « la loi modifiée du 25 mars 2020 »).
 8. Selon l'exposé des motifs du projet de loi, la loi modifiée du 25 mars 2020 adapte la législation luxembourgeoise aux exigences européennes en matière de transparence des personnes morales qui découlent de l'article 1^{er}, points 19 et 29 de la directive (UE) 2018/843 du Parlement européen et du Conseil du 30 mai 2018 (dénommée ci-après « directive (UE) 2018/843 » ou « 5^{ème} directive AML ») modifiant la directive (UE) 2015/849 du Parlement européen et du Conseil du 20 mai 2015 (dénommée ci-après « directive (UE) 2015/849 » ou « 4^{ème} directive AML ») relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme ainsi que les directives 2009/138/CE et 2013/36/UE. Cette loi parachève ainsi la transposition de la 5^{ème} directive AML.
 9. La première partie de la loi modifiée du 25 mars 2020 (Titre I^{er}) institue un système électronique central de recherche de données concernant des comptes de paiement et des comptes bancaires identifiés par un numéro IBAN et des coffres-forts tenus par des établissements de crédit au Luxembourg et apporte des modifications ciblées à la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme (ci-après « loi relative à la lutte contre le blanchiment et contre le financement du terrorisme »).
 10. Le Titre II de la loi modifiée du 25 mars 2020 prévoit quant à lui l'introduction de dispositions particulières applicables aux prestataires de services d'actifs virtuels (ci-après, les « PSAV ») et aux prestataires de services aux sociétés et fiducies (ci-après, les « PSSF »). Le texte prévoit notamment une obligation d'enregistrement auprès de la CSSF pour les PSAV et auprès des autorités de contrôle ou organismes d'autorégulation pour les PSSF. Les dispositions en question prévoient également la mise en place d'un registre des PSAV par la CSSF et d'une liste des PSSF par les autorités de contrôle et les organismes d'autorégulation.

Remarques liminaires

11. Dans le cadre de la transposition de l'article 1^{er}, point 19 de la 5^{ème} Directive AML, les rédacteurs de la loi modifiée du 25 mars 2020 ont décidé de la mise en place d'un système électronique central de recherche de données basé sur les fichiers mis en place par les professionnels. Un tel système de recherche basé sur des fichiers décentralisés permet ainsi d'avoir une vue d'ensemble des comptes détenus par une personne concernée au Luxembourg. La CNPD accueille favorablement ce choix, cette mesure présentant moins d'ingérence dans la vie privée que la création d'un registre central.

12. La lutte contre le blanchiment de capitaux et le financement du terrorisme constitue une priorité en matière de sécurité des citoyens européens en veillant à ce que le système financier soit sûr et fiable. Sans remettre en cause la nécessité de mettre en place des outils de surveillance et d'analyse appropriés et opérationnels, aidant ainsi à détecter les types de transaction suspects, contribuer à une meilleure compréhension des connexions, réseaux et menaces terroristes et criminels et permettre à toutes les autorités compétentes concernées de prendre des mesures préventives adéquates, la CNPD souligne néanmoins le caractère sensible d'un tel système de recherche de données par rapport aux droits et libertés des personnes concernées.
13. En effet, ce système permet de recenser toutes les personnes détenant un compte de paiement ou bancaire ou un coffre-fort tenu par un établissement de crédit au Luxembourg, couvrant de fait non seulement la quasi-majorité des citoyens luxembourgeois mais également tous les clients non-résidents.
14. L'article 6, paragraphe 2 du RGPD dispose que si le traitement est nécessaire au respect d'une obligation légale ou à l'exécution d'une mission d'intérêt public – comme c'est le cas avec le système de recherche mis en place par la loi modifiée du 25 mars 2020 –, les Etats membres peuvent introduire des dispositions plus spécifiques, en déterminant plus précisément les exigences spécifiques applicables au traitement, ainsi que d'autres mesures visant à garantir un traitement licite et loyal.
15. La CNPD rappelle également que la protection des données à caractère personnel constitue au niveau national une matière réservée à la loi en ce qu'elle touche à la protection de la vie privée des citoyens (article 11 paragraphe (3) de la Constitution). En vertu de l'article 32, paragraphe (3) de la Constitution, dans lesdites matières réservées à la loi par la Constitution, « *le Grand-Duc ne peut prendre des règlements et arrêtés qu'en vertu d'une disposition légale particulière qui fixe, outre les objectifs, les principes et points essentiels des mesures d'exécution.* »³. Les éléments essentiels⁴, les objectifs et les principes⁵ doivent dès lors figurer dans la loi au sens stricte du terme.
16. En prévision de l'entrée en vigueur de la révision constitutionnelle le 1^{er} juillet 2023, il est intéressant de noter que l'article 31 de la Constitution révisée dispose que « *[t]oute personne a droit à l'autodétermination informationnelle et à la protection des données à caractère personnel la concernant. Ces données ne peuvent être traitées qu'à des fins et dans les conditions déterminées par la loi.* » Aux termes de l'article 45, paragraphe 2 de la Constitution révisée, « *[d]ans les matières réservées à la loi par la Constitution, le Grand-Duc ne peut prendre des règlements et arrêtés qu'en vertu d'une disposition légale particulière qui fixe l'objectif des mesures d'exécution et le cas échéant les conditions auxquelles elles sont soumises* ».

³ Avis n° 52976 du Conseil d'Etat du 24 juillet 2018 relatif au Projet de règlement grand-ducal 1. modifiant le règlement grand-ducal modifié du 10 août 2005 relatif au fonctionnement du lycée-pilote, et 2. abrogeant le règlement grand-ducal du 27 août 2012 portant sur les classes de la division supérieure de l'enseignement secondaire dans le cycle de formation du lycée Ermesinde

⁴ Arrêt de la Cour constitutionnelle - Arrêts n° 00132 et 00133 du 2 mars 2018

⁵ Avis n° 52976 du Conseil d'Etat du 24 juillet 2018 relatif au Projet de règlement grand-ducal 1. modifiant le règlement grand-ducal modifié du 10 août 2005 relatif au fonctionnement du lycée-pilote, et 2. abrogeant le règlement grand-ducal du 27 août 2012 portant sur les classes de la division supérieure de l'enseignement secondaire dans le cycle de formation du lycée Ermesinde



17. Au vu de ce qui précède, la CNPD regrette que la loi modifiée du 25 mars 2020 ne contienne pas davantage de dispositions précisant les conditions d'application des règles relatives à la protection des données à caractère personnel. En présence d'une atteinte aux droits et libertés fondamentaux des citoyens, la loi modifiée du 25 mars 2020 devrait être plus précise sur les éléments essentiels de la mesure en place, en précisant par exemple les qualifications des différents acteurs impliqués dans le traitement (responsables de traitement et sous-traitants) ou encore les modalités d'application des droits des personnes concernées et leurs éventuelles limitations.

I. Quant à l'application du RGPD

18. La Commission nationale accueille avec intérêt les dispositions du Chapitre 5 du Titre 1^{er} relatives au traitement des données à caractère personnel, notamment la précision par rapport à l'application du RGPD au traitement mis en place par la loi modifiée du 25 mars 2020, à savoir un système électronique central de recherche de données basé sur les fichiers mis en place par les professionnels.
19. Toutefois, la CNPD attire l'attention des auteurs de la loi modifiée du 25 mars 2020 sur le considérant 40 de la 5^{ème} Directive AML qui précise que « *La présente directive est sans préjudice de la protection des données à caractère personnel traitées par les autorités compétentes conformément à la directive (UE) 2016/680* » et recommande l'introduction d'une disposition similaire dans la loi modifiée du 25 mars 2020.

En effet, la Commission nationale tient à rappeler l'applicabilité des dispositions spécifiques de la loi du 1^{er} août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale (ci-après « la loi du 1^{er} août 2018 en matière pénale ainsi qu'en matière de sécurité nationale ») lorsque « *toute autorité publique compétente ou tout autre organisme ou entité à qui a été confié, à ces mêmes fins, l'exercice de l'autorité publique et des prérogatives de puissance publique* » est amenée à avoir recours au système électronique central de recherche de données pour des « *traitements de données à caractère personnel mis en œuvre à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces* ». Ces dispositions spéciales ont vocation à s'appliquer notamment aux autorités nationales suivantes:

- au procureur général d'Etat, aux procureurs d'Etat ainsi qu'aux membres de leurs parquets ;
- aux juges d'instruction ;
- à la Cellule de renseignement financier, dénommée ci-après « CRF » ;
- aux agents de police judiciaire et officiers de police judiciaire affectés au Service de police judiciaire, ainsi qu'aux officiers de police judiciaire visés à l'article 10 du Code de procédure pénale et agréés par le directeur général de la Police grand-ducale ;

- au Service de renseignement de l'Etat.

20. Dans un souci de sécurité juridique, la CNPD souligne la nécessité de préciser dans la loi que deux régimes de protection des données à caractère personnel peuvent s'appliquer aux différentes hypothèses de traitement prévues dans la loi modifiée du 25 mars 2020. Elle recommande alors l'ajout d'une disposition telle que la suivante : « *La présente disposition est sans préjudice de la protection des données à caractère personnel traitées par les autorités compétentes conformément à la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale.* »

II. Quant à la finalité des traitements

21. En vertu de l'article 5, paragraphe 1 (b) du RGPD, les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités.
22. Il ressort de l'exposé des motifs du projet de loi que le système électronique central de recherche de données a pour finalité générale de permettre aux autorités nationales et aux organismes d'autorégulation de rechercher des données dans le cadre de leurs missions et enquêtes en matière de lutte contre le blanchiment et le financement du terrorisme. L'objectif recherché est de leur donner un accès en temps utile, de manière non fragmentée, aux informations sur l'identité des titulaires de comptes bancaires et de comptes de paiement, de leurs mandataires et de leurs bénéficiaires effectifs ainsi que des locataires de coffres-forts.
23. C'est ce que précise également le considérant 20 de la 5^{ème} Directive AML : « *Des retards dans l'accès des CRF et des autres autorités compétentes aux informations sur l'identité des titulaires de comptes bancaires et de comptes de paiement ainsi que de coffres-forts, en particulier ceux qui sont anonymes, entravent la détection des transferts de fonds liés au terrorisme. Les données nationales permettant l'identification des comptes bancaires et des comptes de paiement ainsi que des coffres-forts appartenant à une même personne sont fragmentées et ne sont donc pas accessibles en temps utile aux CRF et aux autres autorités compétentes. Il est dès lors indispensable de mettre en place des mécanismes centralisés automatisés tels qu'un registre ou un système de recherche de données dans tous les États membres, qui constituent des moyens efficaces d'obtenir un accès en temps utile aux informations sur l'identité des titulaires de comptes bancaires et de comptes de paiement ainsi que de coffres-forts, de leurs mandataires et de leurs bénéficiaires effectifs. Lors de l'application des modalités d'accès, il convient d'utiliser les mécanismes existants, pour autant que les CRF nationales puissent avoir accès, immédiatement et sans filtrage, aux données pour lesquelles elles procèdent à des enquêtes. (...)* ».
24. La CNPD souligne toutefois qu'il convient de distinguer les différentes finalités pour lesquelles chacune des entités respectives visées par la loi modifiée du 25 mars 2020 traitent des données à caractère personnel. Comme évoqué ci-après ('Point III. Les rôles et les responsabilités'), les



professionnels mettent en place les fichiers afin de répondre à leurs propres obligations légales pour la prévention du blanchiment et du financement du terrorisme. Quant à la CSSF, celle-ci met en place le système électronique central de recherche de données afin de permettre aux autorités nationales (dont la CSSF elle-même) de rechercher des données dans le cadre de leurs missions et enquêtes en matière de lutte contre le blanchiment et le financement du terrorisme. Néanmoins, la Commission nationale observe qu'une distinction entre le traitement par la CSSF pour la gestion du système de recherche (auquel cas elle bénéficie d'un accès direct en vertu de l'article 7, paragraphe 2) et le traitement par la CSSF qui accède aux données via le système de recherche dans le cadre de ses missions de surveillance en matière de lutte contre le blanchiment et le financement du terrorisme (auquel cas elle bénéficie d'un accès indirect en vertu de l'article 8, paragraphe 2) doit être opérée. Une distinction claire des finalités est primordiale, notamment au stade de la mise en place de mesures organisationnelles de sécurité (cf. 'VII. Quant aux mesures de sécurité').

25. La CNPD note qu'avec les modifications introduites par la loi du 28 octobre 2022 portant création de la procédure de dissolution administrative sans liquidation et la loi du 16 mai 2023 relative à l'échange automatique et obligatoire des informations déclarées par les Opérateurs de Plateforme, les finalités du système électronique central de recherche de données ont été élargies :

- afin de permettre l'identification, par le gestionnaire du Registre de commerce et des sociétés, des comptes de paiement, des comptes bancaires ou des coffres-forts qui sont ouverts au nom de la société commerciale qui fait l'objet d'une procédure de dissolution administrative sans liquidation ;
- aux fins des missions de l'Administration des contributions directes en matière de coopération administrative dans le domaine fiscal qui découlent de la loi modifiée du 29 mars 2013 relative à la coopération administrative dans le domaine fiscal et de la loi modifiée du 18 décembre 2015 relative à la Norme commune de déclaration (NCD) ;
- aux fins des missions de l'AED et l'Administration des douanes et accises en matière d'assistance mutuelle en matière de recouvrement qui découlent de la loi modifiée du 21 juillet 2012 concernant l'assistance mutuelle en matière de recouvrement des créances relatives aux taxes, impôts, droits et autres mesures dans l'Union européenne, l'Administration des contributions directes.

26. Par ailleurs, la limitation des finalités est également un aspect important à prendre en compte dans le cadre du système d'échange d'informations entre les différentes cellules de renseignement financier des pays membres de l'Union Européenne⁶ et de l'interconnexion des mécanismes automatisés centralisés telle que prévu dans l'article 32 bis, paragraphe 5 de la 4^{ème} Directive AML. Dans son rapport du 24 juillet 2019 sur l'interconnexion des mécanismes automatisés centralisés nationaux (registres centraux ou systèmes électroniques centraux de

⁶ Cf. Directive (UE) 2019/1153 du Parlement européen et du Conseil du 20 juin 2019 fixant les règles facilitant l'utilisation d'informations financières et d'une autre nature aux fins de la prévention ou de la détection de certaines infractions pénales, ou des enquêtes ou des poursuites en la matière, et abrogeant la décision 2000/642/JAI du Conseil

recherche de données) des États membres concernant les comptes bancaires, la Commission Européenne a indiqué à ce propos que « conformément aux règles de protection des données, l'accès aux données à caractère personnel devrait être proportionné à ce qui est nécessaire à la réalisation des objectifs définis dans la directive anti-blanchiment »⁷.

27. Enfin, la Commission nationale rappelle que la consultation concrète de données à caractère personnel dans le système électronique central de recherche de données doit toujours passer le test du principe de finalité et de proportionnalité. Cela implique, pour chaque personne habilitée, à n'effectuer des recherches sur ce système que lorsqu'un tel accès est adéquat, pertinent et nécessaire à la lumière des tâches légales spécifiques pour lesquelles elle a obtenu cet accès.

III. Les rôles et les responsabilités

28. La CNPD constate à regret que la loi modifiée du 25 mars 2020 ne désigne pas le(s) responsable(s) de traitement comme cela est par exemple le cas dans la loi modifiée du 13 janvier 2019 instituant un Registre des bénéficiaires effectifs, transposant l'article 30 de la 4^{ème} Directive AML. En vertu du principe de responsabilisation, qui se traduit par l'obligation pour une organisation de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données, il est essentiel qu'un ou des responsable(s) de traitement soi(en)t identifié(s)⁸.
29. Dans le cadre de la présente loi, afin de transposer l'article 1^{er}, point 19 de la 5^{ème} Directive AML, les rédacteurs ont fait le choix d'un système électronique central de recherche de données basé sur les fichiers mis en place par les professionnels (et non d'un registre central). Les données en question ne font pas l'objet d'un stockage centralisé auprès de la CSSF (données en transit sur le système électronique central de recherche). La Circulaire CSSF 20/747 précise que « sur base journalière, le professionnel doit constituer dans son système informatique les fichiers de données concernant toute information relative aux comptes de paiement, aux comptes bancaires et/ou aux coffres-forts ». Dans un deuxième temps, « le professionnel met à disposition le fichier et prévient la CSSF de sa disponibilité ». Puis, « la CSSF se connecte et télécharge le fichier ». Enfin, « la CSSF envoie aux professionnels un fichier de retour (feedback) incluant le statut du fichier téléchargé : accepté ou rejeté incluant les erreurs rencontrées »⁹.
30. Au vu de la configuration choisie, il conviendrait d'analyser les traitements de données mis en place par la loi modifiée du 25 mars 2020 et de s'interroger sur le rôle des différentes entités impliquées.
31. D'une part, il est prévu dans la loi modifiée du 25 mars 2020 que les professionnels :

⁷ COM(2019) 372 final

⁸ Avis 1/2017 du CEPD sur la proposition de la Commission modifiant la directive (UE) 2015/849 et la directive 2009/101/CE

⁹ https://www.cssf.lu/wp-content/uploads/cssf20_747.pdf



- mettent en place un fichier de données et de conservation de données permettant l'identification de toute personne physique ou morale qui détient ou contrôle des comptes de paiement ou des comptes bancaires identifiés par un numéro IBAN, ainsi que des coffres-forts (article 2, paragraphe 1);
- collectent les données énumérées dans la loi du 25 mars 2020 (article 2, paragraphe 1);
- mettent à jour ces données (article 2, paragraphe 2);
- soient responsables de leur propre fichier (article 2, paragraphe 4);
- mettent en place, à leurs frais, toutes les mesures nécessaires pour assurer l'accès à leurs fichiers par la CSSF, dont certaines mesures de sécurité (article 2, paragraphe 4).

32. D'autre part, il est prévu dans la loi modifiée du 25 mars 2020 que la CSSF :

- mette en place et assure la gestion du système électronique central de recherche de données (article 7, paragraphe 1);
- accède aux fichiers de données des professionnels (article 7, paragraphe 2);
- définisse la structure du fichier et le détail des données (article 2, paragraphe 4);
- arrête la procédure de demande de communication des données des fichiers aux autorités nationales et aux organismes d'autorégulation et transmette des données à ceux-ci (article 8, paragraphe 2);
- arrête la procédure relative à l'acquisition et à la mise à jour du matériel nécessaire pour assurer la confidentialité et la sauvegarde du secret professionnel dans les fichiers mis en place par les professionnels, ainsi que la protection contre les accès non autorisés, l'installation d'une liaison de télécommunication adéquate et la participation au système utilisateur fermé, ainsi que la fourniture continue desdits services au moyen de ces installations (article 2, paragraphe 4);
- mette en place des mesures techniques et organisationnelles permettant de garantir la sécurité des données accessibles par le système électronique central de recherche (article 9, paragraphe 1);
- référence les accès aux données accessibles par le système électronique central de recherche (article 9, paragraphes 2 et 3).

33. L'article 4, point 7 du RGPD définit le responsable du traitement comme « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement.* ». Cette disposition précise également que « *lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre* ».

La CNPD estime nécessaire de préciser que dans le cas d'une entité publique, c'est bien en vertu de la loi que celle-ci est chargée de certaines tâches administratives. Ce n'est donc pas l'entité publique désignée qui détermine elle-même les finalités et les moyens du traitement de données à caractère personnel mais les dispositions légales mettant en place le traitement. Il appartient

donc au texte de loi de déterminer qui sont les responsables de traitement. Au vu de la répartition des tâches que met en place la loi modifiée du 25 mars 2020 et des finalités énoncées dans le Point II du présent avis, la Commission nationale est en faveur de la qualification de la CSSF et de chaque professionnel comme responsables de traitement séparés, chaque entité étant respectivement responsable pour le traitement qui lui incombe et qu'elle met en place.

34. En outre, l'article 2, paragraphe 5 prévoit la possibilité pour le professionnel de déléguer ses obligations. Une telle délégation constitue une relation de sous-traitance au sens de l'article 28 du RGPD, ce qui implique un certain nombre d'obligations pour le professionnel agissant comme responsable de traitement, avec notamment la mise en place d'un contrat de sous-traitance définissant l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et les obligations et les droits du responsable du traitement. La CNPD recommande, à l'instar des renvois aux articles 41, paragraphe 2bis, de la Loi du 5 avril 1993 relative au secteur financier telle qu'elle a été modifiée et 30, paragraphe 2bis, de la Loi du 10 novembre 2009 relative aux services de paiement, l'insertion d'une référence à l'article 28 du RGPD.

IV. Quant aux données traitées

35. La Commission nationale note que l'article 2, paragraphe 1 transpose le paragraphe 3 de l'article 32bis de la 4^{ème} Directive AML relatif aux informations accessibles et pouvant faire l'objet de recherches au moyen des mécanismes centralisés. La loi modifiée du 25 mars 2020 précise ainsi que les fichiers des professionnels comprennent les données suivantes :

*« a) les données relatives à tout titulaire d'un compte client et toute personne prétendant agir au nom du client, à savoir le nom, complété par les autres données d'identification requises au titre de l'article 3, paragraphe 2, lettre a), de la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme ;
b) les données relatives au bénéficiaire effectif du titulaire d'un compte client, à savoir le nom, complété par les autres données d'identification requises au titre de l'article 3, paragraphe 2, lettre b), de la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme ;
c) les données relatives au compte bancaire ou au compte de paiement, à savoir le numéro IBAN et la date d'ouverture et de clôture du compte ; et
d) les données relatives au coffre-fort, à savoir le nom du locataire, complété par les autres données d'identification requises au titre de l'article 3, paragraphe 2, de la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme, ainsi que la durée de la période de location.*

Ces données peuvent être complétées par un numéro d'identification unique.»

36. L'article 3, paragraphe 2, lettre a), de la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme concerne « *l'identification du client et la vérification de son identité, sur la base de documents, de données ou d'informations de « sources fiables et indépendantes [...] »*. L'article 16 du Règlement CSSF N° 12-02 du 14 décembre 2012 relatif à la lutte contre le blanchiment et contre le financement du terrorisme vient préciser que les professionnels doivent recueillir, en ce qui concerne les clients qui sont des personnes physiques: « *[...] nom(s) et prénom(s) ; lieu et date de naissance ; nationalité(s) ; adresse postale complète de la résidence principale du client ; le cas échéant, le numéro d'identification national officiel.* »
37. D'une part, la CNPD s'interroge sur la définition de la notion de « numéro d'identification unique » dans la loi modifiée du 25 mars 2020 et si cette notion se recoupe avec celle de « numéro d'identification national ».
38. D'autre part, il ressort de l'article 32bis, paragraphe 3 de la 4^{ème} Directive AML que les informations à conserver sont « *le nom, complété soit par les autres données d'identification requises au titre des dispositions nationales transposant l'article 13, paragraphe 1, point a), soit par un numéro d'identification unique* ». La Commission nationale se demande alors si la loi modifiée du 25 mars 2020 ne va pas au-delà des données considérées comme étant strictement nécessaires par la 4^{ème} Directive AML puisqu'elle laisse la possibilité au professionnel d'inclure le numéro d'identification national officiel (dans le cadre du renvoi à l'article 3, paragraphe 2, lettre a) de la loi modifiée du 12 novembre 2004 et à l'article 16 du Règlement CSSF N° 12-02 du 14 décembre 2012) et un numéro d'identification unique. En effet, la 4^{ème} Directive AML n'exige pas la conservation du numéro d'identification unique ensemble avec les autres données d'identification requises au titre des dispositions nationales transposant l'article 13, paragraphe 1, point a) de la directive. Alors que la directive permet aux Etats-membres de prévoir un accès à « *d'autres informations jugées essentielles aux CRF et aux autres autorités compétentes* », le commentaire du projet de loi ne précise pas la nécessité de cette information supplémentaire.
39. Le RGPD (article 5, paragraphe 1 (c)) prévoit que les données doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (principe de minimisation des données). Ce principe implique que le responsable de traitement ne traite que les données qui sont nécessaires (et non seulement utiles) à la réalisation des finalités.
40. A cet égard, la CNPD souhaite également rappeler le considérant 21 de la 5^{ème} Directive AML prévoyant que « *les données minimales nécessaires à la réalisation des enquêtes dans le cadre de la lutte contre le blanchiment de capitaux et le financement du terrorisme devraient être conservées dans des mécanismes automatisés centralisés pour les comptes bancaires et les comptes de paiement, tels que des registres ou des systèmes de recherche de données.* ». Ce principe ressort également du rapport de la Commission Européenne du 24 juillet 2019 sur l'interconnexion des mécanismes automatisés centralisés nationaux (registres centraux ou systèmes électroniques centraux de recherche de données) des États membres concernant les comptes bancaires, dans lequel elle a précisé que « *du point de vue de la protection des données*

à caractère personnel, il semble nécessaire de restreindre la portée des informations consultables via la plateforme d'interconnexion à l'ensemble minimal obligatoire d'informations tel que défini à l'article 32 bis, paragraphe 3, de la directive anti-blanchiment »¹⁰.

41. Afin de respecter le principe de minimisation des données et dans un souci de sécurité juridique, la loi modifiée du 25 mars 2020 devrait se limiter à prévoir l'obligation de conserver soit le numéro d'identification unique, soit les autres données d'identification requises au titre de l'article 3, paragraphe 2, lettre (a), de la loi relative à la lutte contre le blanchiment et contre le financement du terrorisme.
42. Par ailleurs, la CSSF semble avoir interprété la notion de « numéro d'identification unique » de manière extensive dans le sens où tout identifiant connu devrait être indiqué (cf. annexe 2 de la Circulaire 20/747 qui fait référence au NIN (Numéro d'Identification Nationale), au TIN (Numéro d'Identification Fiscale), mais également au numéro de passeport, de carte d'identité, de permis de conduire ou encore un identifiant unique utilisé pour identifier le compte à l'intérieur du fichier, tout en indiquant que « *toutes les informations connues doivent être renseignées* »)¹¹. Une telle collecte, même si elle était optionnelle, contrevient au principe de minimisation des données prévu à l'article 5, paragraphe 1 (c)) du RGPD.
43. En outre, il ressort de l'article 2, paragraphe 1^{er}, lettre (a) de la loi modifiée du 25 mars 2020 que les professionnels doivent mettre en place un fichier de données permettant l'identification de « *tout titulaire d'un compte client et toute personne prétendant agir au nom du client* ». Or, la loi modifiée du 25 mars 2020 ne fournit pas de définition claire des termes « *toute personne prétendant agir au nom du client* ». La CNPD constate que le texte de loi reprend les termes de l'article 32 bis, paragraphe 3 de la 4^{ème} Directive telle que modifiée par la 5^{ème} Directive (article 1^{er}, point 19 de la 5^{ème} Directive AML). Le commentaire de l'article 2 dans le projet de loi précise qu'il faut entendre, notamment, les mandataires détenant une procuration d'un client personne morale leur donnant le pouvoir d'agir en son nom et les mandataires/fondés de procuration d'un client personne physique. Néanmoins, afin d'assurer la protection des données des personnes concernées et permettre aux professionnels d'identifier avec certitude ces dernières, la Commission nationale rejoint l'avis de la Chambre de Commerce¹² sur ce point et recommande de préciser clairement ces termes dans la loi.
44. Par ailleurs, le commentaire de l'article 2, paragraphe 2, du projet de loi devenu la loi modifiée du 25 mars 2020 précise que les données des clients doivent être mises à jour en vertu des obligations de vigilance constante des professionnels conformément à la loi relative à la lutte contre le blanchiment et contre le financement du terrorisme et qu'en cas de modification des données, les professionnels devront s'assurer que ces changements sont répercutés dans le fichier dans un délai raisonnable qui ne dépasse pas un jour. Ces obligations sont en ligne avec le respect du principe d'exactitude énoncé à l'article 5, paragraphe 1 (d) du RGPD et avec l'article 19 du RGPD qui prévoit que « *Le responsable du traitement notifie à chaque destinataire auquel*

¹⁰ COM(2019) 372 final

¹¹ <https://www.cssf.lu/fr/document/annexe-2-de-la-circulaire-cssf-20-747/>

¹² Avis de la Chambre de Commerce du 7 février 2020 sur le projet de loi n°7512



les données à caractère personnel ont été communiquées toute rectification ou tout effacement de données à caractère personnel ou toute limitation du traitement [...] ». Dans ce contexte, la CNPD se félicite de la présence d'une disposition relative au caractère adéquat, exact et actuel des données présentes dans les fichiers de données mis en place par les professionnels.

45. La durée conservation des données des fichiers est prévue par l'article 2, paragraphe 3 de la loi modifiée du 25 mars 2020 qui opère lui-même un renvoi aux dispositions de l'article 3, paragraphe 6 de la loi relative à la lutte contre le blanchiment et contre le financement du terrorisme. A ce titre, la Commission nationale renvoie les auteurs de la loi modifiée du 25 mars 2020 à ses observations formulées à propos de ces dispositions dans ses avis du 18 janvier 2018 à propos du projet de loi n°7128¹³ et du 28 février 2020 à propos du projet de loi n°7467¹⁴.

V. Quant aux modalités d'accès et de recherche

46. La Commission nationale rappelle que le Conseil d'Etat a énoncé à plusieurs reprises que l'accès à des fichiers externes et la communication de données informatiques à des tiers constituent une ingérence dans la vie privée et partant, en vertu de l'article 11, paragraphe 3, de la Constitution, une matière réservée à la loi formelle¹⁵. Les éléments essentiels¹⁶, dont notamment les modalités d'accès, doivent dès lors figurer dans la loi.
47. Le système électronique central de recherche des données donne un accès direct, immédiat et non filtré aux données des fichiers créés par les professionnels aux personnes habilitées :

¹³ Projet de loi n°7128 portant 1. transposition des dispositions de la directive (UE) 2015/849 du Parlement européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) n° 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission ayant trait aux obligations professionnelles en matière de lutte contre le blanchiment et contre le financement du terrorisme et aux pouvoirs des autorités de contrôle; 2. mise en œuvre du règlement (UE) 2015/847 du Parlement européen et du Conseil du 20 mai 2015 sur les informations accompagnant les transferts de fonds et abrogeant le règlement (CE) n° 1781/2006; 3. modification de: a) la loi modifiée du 9 décembre 1976 relative à l'organisation du notariat; b) la loi modifiée du 4 décembre 1990 portant organisation du service des huissiers de justice; c) la loi modifiée du 10 août 1991 sur la profession d'avocat; d) la loi modifiée du 5 avril 1993 relative au secteur financier; e) la loi modifiée du 10 juin 1999 portant organisation de la profession d'expert-comptable; f) la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme; g) la loi modifiée du 10 novembre 2009 relative aux services de paiement; h) la loi du 21 décembre 2012 relative à l'activité de Family Office; i) la loi modifiée du 7 décembre 2015 sur le secteur des assurances; j) la loi du 23 juillet 2016 relative à la profession de l'audit

¹⁴ Projet de loi n°7467 portant modification de : 1° la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme ; 2° la loi modifiée du 9 décembre 1976 relative à l'organisation du notariat ; 3° la loi modifiée du 4 décembre 1990 portant organisation du service des huissiers de justice ; 4° la loi modifiée du 10 août 1991 sur la profession d'avocat ; 5° la loi modifiée du 10 juin 1999 portant organisation de la profession d'expert-comptable ; 6° la loi modifiée du 23 juillet 2016 relative à la profession de l'audit, en vue de la transposition de certaines dispositions de la directive (UE) 2018/843 du Parlement européen et du Conseil du 30 mai 2018 modifiant la directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme ainsi que les directives 2009/138/CE et 2013/36/UE

¹⁵ Avis du Conseil d'Etat du 23 mai 2017 portant modification de la loi modifiée du 4 juillet 2008 sur la jeunesse et portant modification de la loi du 18 mars 2013 relative aux traitements des données à caractère personnel concernant les élèves , p.17

¹⁶ Arrêt de la Cour constitutionnelle - Arrêts n°00132 et 00133 du 2 mars 2018



- de la CSSF afin de s'acquitter de ses missions en vertu du paragraphe 1^{er} de la loi modifiée du 25 mars 2020 (article 7, paragraphe 2) ;
- de la Cellule de renseignement financier dans le cadre de ses missions (article 8, paragraphe 1) ;
- du Bureau de recouvrement des avoirs dans la mesure où cela est nécessaire à l'accomplissement de ses missions, aux fins d'identifier, de dépister, de geler ou saisir des avoirs liés à une enquête ou des poursuites pour blanchiment, financement du terrorisme ou pour une infraction sous-jacente associée (article 8, paragraphe 1) ;
- de l'Administration des contributions directes aux fins de ses missions en matière de coopération administrative dans le domaine fiscal qui découlent de la loi modifiée du 29 mars 2013 relative à la coopération administrative dans le domaine fiscal et de la loi modifiée du 18 décembre 2015 relative à la Norme commune de déclaration (article 8, paragraphe 1bis);
- de l'Administration des contributions directes, de l'AED et de l'Administration des douanes et accises aux fins de leurs missions en matière d'assistance mutuelle en matière de recouvrement qui découlent de la loi modifiée du 21 juillet 2012 concernant l'assistance mutuelle en matière de recouvrement des créances relatives aux taxes, impôts, droits et autres mesures dans l'Union européenne (article 8, paragraphe 1bis).

48. L'article 8, paragraphe 2 de la loi modifiée du 25 mars 2020 indique quant à lui que les autorités autres que celles visées au paragraphe 1^{er} et les organismes d'autorégulation peuvent, dans la mesure où cela est nécessaire dans l'accomplissement des obligations qui leurs incombent en matière de lutte contre le blanchiment et contre le financement du terrorisme, demander à la CSSF à recevoir sans délai les données. Le gestionnaire du Registre de commerce et des sociétés bénéficie du même type d'accès dans le cadre d'une procédure de dissolution administrative sans liquidation (article 8, paragraphe 2bis).
49. En tout état de cause, la Commission nationale accueille favorablement les dispositions relatives au nombre limité de personnes autorisées au sein des autorités nationales, des organismes d'autorégulation et du gestionnaire du Registre de commerce et des sociétés à accéder au système de recherche et à la communication de listes de ce personnel spécifiquement désigné et autorisé à la CSSF (article 8, paragraphe 3). La CNPD accueille également avec intérêt la mesure relative à la consignation des données relatives à chaque accès et recherche effectuée dans le système de recherche (article 9, paragraphes 2 et 3). La Commission nationale regrette néanmoins que ces aspects ne fassent pas l'objet de précisions dans la Circulaire CSSF 20/747.
50. Toutefois, la Commission nationale note que la loi modifiée du 25 mars 2020 ne fixe pas avec assez de précision les modalités d'accès et de recherches par les autorités nationales, les organismes d'autorégulation et le gestionnaire du Registre de commerce et des sociétés. S'agissant d'une matière réservée à la loi, les éléments essentiels devraient être fixés dans la loi. Ainsi, les modalités d'accès devraient être fixées dans la loi ou dans un règlement grand-

ducal. Afin d'éviter que les recherches par les autorités nationales et les organismes d'autorégulation ne puissent revêtir un caractère exploratoire (« *fishing expeditions* »), constitutives d'une collecte disproportionnée, voire abusive, de données à caractère personnel, la loi devrait par exemple exiger l'indication d'un motif d'accès et préciser les données d'identification devant être communiquées pour procéder à une recherche ciblée dans le système. De telles conditions permettraient d'éviter la possibilité d'effectuer des « recherches approximatives », c'est-à-dire des recherches qui génèrent des plages de résultats plus larges, même si un terme est mal orthographié ou incomplet, élargissant ainsi les résultats de concordances.

VI. Quant aux droits des personnes concernées

51. En application des articles 12, 13, 14, 15 et 16 du RGPD, les personnes concernées doivent être informées de ce que leurs données sont enregistrées et accessibles aux autorités nationales et doivent disposer d'un point de contact pour exercer leurs droits d'accès et de rectification¹⁷.

(a) L'information des personnes concernées

52. Les professionnels, qui collectent les données directement auprès des personnes concernées, ont l'obligation de fournir à ces dernières les informations figurant à l'article 13 du RGPD. Les personnes dont les données à caractère personnel pourraient être utilisées dans le cadre de la lutte contre le blanchiment d'argent et le financement du terrorisme devront donc être informées par le professionnel de la possibilité que leurs données soient utilisées à ces fins via le système électronique central de recherche de données. Les personnes concernées devraient notamment pouvoir aisément identifier les administrations, qui pourraient avoir accès à ce système de recherche.
53. Pour ce qui est de la CSSF, celle-ci collectera les données de manière indirecte et devrait être ainsi soumise aux obligations prévues à l'article 14 du RGPD. Le paragraphe 5, lettre (c) de cet article prévoit que le responsable du traitement est exempté de son obligation d'information, si l'obtention ou la communication est prévue par la loi, qui doit prévoir « *des mesures appropriées visant à protéger les intérêts légitimes de la personne concernée* ». La CNPD estime que de telles mesures peuvent se concrétiser par certaines mesures déjà prévues dans la loi comme la limitation du nombre de personnes autorisées à accéder au système électronique central de recherche de données ou la consignation des accès dans des registres, mais également toutes les mesures préconisées par la CNPD dans cet avis.
54. Cette absence d'information par la CSSF est d'ailleurs en ligne avec le principe de confidentialité énoncé à l'article 2, paragraphe 4 de la loi modifiée du 25 mars 2020 (en ce qui concerne l'accès

¹⁷ Proposition de DIRECTIVE DU PARLEMENT EUROPÉEN ET DU CONSEIL modifiant la directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme et la directive 2009/101/CE <https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52016PC0450&from=EN>

par la CSSF au fichier de données). Ce principe est explicité dans le considérant 20 de la 5^{ème} Directive AML: « Une confidentialité complète devrait être assurée en ce qui concerne ces enquêtes et demandes d'informations y afférentes émanant des CRF et des autorités compétentes autres que celles en charge des poursuites pénales. » Le commentaire des articles précise en effet que le professionnel ne doit en aucun cas contrôler les accès ainsi que les données consultées par la CSSF dans le fichier de données.

(b) Le droit d'accès

55. Le droit d'accès des personnes concernées aux fichiers tenus par les professionnels pourra s'exercer normalement auprès de ces derniers en application de l'article 15 du RGPD, sous réserve d'éventuelles limitations prévues dans la loi. Il peut également s'exercer auprès de la CSSF dans la mesure où celle-ci agit en tant que gestionnaire du système électronique central de recherche de données et responsable du traitement, sous réserve d'éventuelles limitations prévues dans la loi.
56. En ce qui concerne notamment un droit d'accès exercé auprès de la CSSF, la CNPD rappelle que le droit d'accès permet également à la personne concernée de prendre connaissance des « destinataires ou catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, en particulier les destinataires qui sont établis dans des pays tiers ou les organisations internationales » (article 15, paragraphe 1 c) du RGPD). Il convient de préciser que la personne concernée a le droit d'obtenir du responsable du traitement des informations sur les destinataires concrets auxquels les données à caractère personnel la concernant ont été ou seront communiquées¹⁸¹⁹²⁰.
57. Néanmoins, le droit d'accès aux destinataires ou catégories de destinataires doit d'abord prendre en compte la définition de destinataire de l'article 4, paragraphe 9 du RGPD qui est basée sur la divulgation de données personnelles à une personne physique ou morale, une autorité publique, un service ou tout autre organisme. Il ressort de cette disposition que les autorités publiques « qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un État membre ne sont pas considérées comme des destinataires »²¹.

¹⁸ Arrêt de la CJUE du 12 janvier 2023, RW contre Österreichische Post AG, C-154/21, para. 46

¹⁹ Arrêt de la CJUE du 12 janvier 2023, RW contre Österreichische Post AG, C-154/21, para. 43 : « Partant, il convient de considérer que les informations fournies à la personne concernée au titre du droit d'accès prévu à l'article 15, paragraphe 1, sous c), du RGPD doivent être les plus exactes possibles. En particulier, ce droit d'accès implique la possibilité pour la personne concernée d'obtenir de la part du responsable du traitement les informations sur les destinataires spécifiques auxquels les données ont été ou seront communiquées ou, alternativement, de choisir de se borner à demander des informations concernant les catégories de destinataires. »

²⁰ EDPB Guidelines 01/2022 on data subject rights - Right of access, Version 2.0, Adopted on 28 March 2023: « Under Article 15, if the data subject has not chosen otherwise, the controller is obliged to name the actual recipients, unless it is impossible to identify those recipients or the controller demonstrates that the data subject's requests for access are manifestly unfounded or excessive within the meaning of Article 12(5) GDPR. » (§117)

²¹ EDPB Guidelines 01/2022 on data subject rights - Right of access, Version 2.0, Adopted on 28 March 2023, §116



58. Au vu de ces précisions apportées par la jurisprudence de la Cour de Justice de l'Union Européenne et par le Comité Européen de la Protection des Données (CEPD), une personne concernée devrait, en principe, pouvoir obtenir une liste précise des entités ayant consulté ou ayant obtenu communication de ses données à moins que ces entités ne soient des autorités publiques agissant dans le cadre d'une mission d'enquête particulière (par exemple en matière de lutte contre le blanchiment et contre le financement du terrorisme, en matière de recouvrement des créances relatives aux taxes, impôts, droits et autres mesures dans l'Union européenne ou en matière de coopération administrative dans le domaine fiscal). La CNPD en déduit que, pour les traitements prévus par la loi faisant l'objet du présent avis, les organismes d'autorégulation et le gestionnaire du Registre de commerce et des sociétés (*Luxembourg Business Registers* ou LBR) sont dans tous les cas à considérer comme destinataires au sens de l'article 4, paragraphe 9 du RGPD.
59. Des exceptions au principe du droit d'accès de la personne concernée peuvent néanmoins être prévues dans le cadre de l'article 23 du RGPD. La Commission nationale note qu'en vertu de l'article 3, paragraphe 6*bis* de la loi relative à la lutte contre le blanchiment et contre le financement du terrorisme, le droit d'accès prévu à l'article 15 du RGPD peut être limité « *en application de l'article 5, paragraphe (5), alinéa 1* [de la loi relative à la lutte contre le blanchiment et contre le financement du terrorisme]», afin de « *a) permettre au professionnel, à la cellule de renseignement financier, à une autorité de contrôle ou à un organisme d'autorégulation d'accomplir ses tâches comme il convient aux fins de la présente loi ou des mesures prises pour son exécution ; ou b) éviter de faire obstacle aux demandes de renseignements, analyses, enquêtes ou procédures à caractère officiel ou judiciaire, menées aux fins de la présente loi, des mesures prises pour son exécution ou de la directive (UE) 2015/849 et pour ne pas compromettre la prévention et la détection des cas de blanchiment ou de financement du terrorisme ni les enquêtes en la matière.* ». La CNPD réitère ses remarques faites dans son avis du 28 février 2020 relatif au projet de loi n° 7467²² et observe qu'il ne ressort pas clairement de l'article 3, paragraphe 6*bis* de la loi relative à la lutte contre le blanchiment et contre le financement du terrorisme si les limitations au droit d'accès prévues dans cette disposition ont vocation à s'appliquer uniquement aux professionnels ou à tout responsable de traitement impliqué dans un traitement sur base de la loi relative à la lutte contre le blanchiment et contre le financement du terrorisme, à savoir également les autorités nationales, dont notamment la CSSF qui gère le système de recherche.

²² Avis de la Commission Nationale pour la Protection des Données du 28 février 2020 relatif au projet de loi n°7467 portant modification de : 1° la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme ; 2° la loi modifiée du 9 décembre 1976 relative à l'organisation du notariat ; 3° la loi modifiée du 4 décembre 1990 portant organisation du service des huissiers de justice ; 4° la loi modifiée du 10 août 1991 sur la profession d'avocat ; 5° la loi modifiée du 10 juin 1999 portant organisation de la profession d'expert-comptable ; 6° la loi modifiée du 23 juillet 2016 relative à la profession de l'audit, en vue de la transposition de certaines dispositions de la directive (UE) 2018/843 du Parlement européen et du Conseil du 30 mai 2018 modifiant la directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme ainsi que les directives 2009/138/CE et 2013/36/UE

60. Si tel n'était pas le cas, au vu des mesures de confidentialité évoquées ci-dessus, qui visent à ne pas compromettre l'efficacité des mesures prévues en matière de lutte contre le blanchiment de capitaux et de financement du terrorisme, les limitations - si elles sont basées sur l'article 23 du RGPD - et les garanties pour les personnes concernées, devraient être prévues par un texte de loi.
61. A cet égard, on peut citer le considérant 46 de la 4^{ème} Directive AML qui énonce qu'en cas d'exceptions ou de limitations au droit d'accès pour éviter de nuire gravement à l'efficacité de la lutte contre le blanchiment de capitaux et le financement du terrorisme, « *La personne concernée a le droit de demander qu'une autorité de contrôle visée à l'article 28 de la directive 95/46/CE ou, le cas échéant, le Contrôleur européen de la protection des données vérifie la licéité du traitement et a le droit de former le recours juridictionnel visé à l'article 22 de ladite directive.* »
62. Les limitations - si elles sont basées sur l'article 23 du RGPD - et les garanties pour les personnes concernées, comme par exemple la possibilité d'obtenir un accès indirect aux données les concernant auprès de la Commission nationale pour la protection des données, doivent donc être prévues par un texte de loi.

(c) Le droit de rectification

63. Au vu du fonctionnement du système électronique de recherche, la CNPD considère que le droit de rectification ne pourra s'effectuer uniquement auprès de chaque professionnel, l'exactitude des données traitées par la CSSF et les autres autorités étant assurée par l'article 2, paragraphe 2 de la loi modifiée du 25 mars 2020 : « *Les données visées au paragraphe 1er sont adéquates, exactes et actuelles. Le fichier de données visé au paragraphe 1er est mis à jour sans délai après toute modification notifiée au ou constatée par le professionnel.* »

VII. Quant aux mesures de sécurité

64. La loi modifiée du 25 mars 2020 prévoit que le professionnel met en place, à ses frais, toutes les mesures nécessaires pour assurer l'accès par la CSSF au fichier de données qui est sous sa responsabilité, dont des mesures pour assurer la confidentialité et la sauvegarde du secret professionnel ainsi que la protection contre les accès non autorisés (article 2, paragraphe 4).
65. Il est par ailleurs prévu que la CSSF accède aux données des fichiers au moyen d'une procédure sécurisée et par un personnel désigné (article 7, paragraphe 2). La CSSF devra mettre en place, conformément à des normes technologiques élevées, des mesures techniques et organisationnelles permettant de garantir la sécurité des données accessibles par le système électronique central de recherche afin de veiller à ce que seules les personnes habilitées aient accès aux données accessibles par le système électronique central de recherche (article 9, paragraphe 1).

66. La sécurité étant primordiale dans la création d'un traitement tel que celui mis en place, la Commission nationale salue le rappel aux principes essentiels en matière de sécurité et les précisions apportées dans l'Annexe 1 de la Circulaire CSSF 20/747 relative aux modalités techniques que les professionnels sont appelés à suivre strictement, notamment dans la section « 4.1.3 Sécurité des fichiers ».
67. La CNPD se félicite des dispositions relatives à la limitation du nombre de personnes autorisées à accéder au système électronique central de recherche de données ou à demander la réception des données, et à la formation spécifique de ce personnel, y compris en matière de protection des données à caractère personnel (article 8, paragraphe 3).
68. Concernant le traçage de toutes les personnes ayant demandé accès aux données et de toutes les recherches effectuées sur base de ces données (mesure prévue à l'article 9, paragraphes 2 et 3), la CNPD comprend que ces données seraient couvertes par les mesures de confidentialité s'imposant aux professionnels (en application de l'article 2, paragraphe 4) et que toute demande d'information et d'accès portant sur ce type de données devrait pouvoir être limitée au risque de compromettre la finalité du traitement mis en place (cf. infra). La Commission nationale remarque toutefois que la liste des éléments devant être mentionnés dans les registres (article 9, paragraphes 2 et 3) devraient comprendre également le motif de consultation, la référence du dossier ne suffisant pas afin de garantir le respect des principes de finalité et de proportionnalité.
69. La CNPD rappelle qu'au sein de la CSSF, seuls les employés ayant la finalité du traitement dans leurs compétences sont habilités à traiter les données collectées à cette fin. Dans la mesure où la CSSF poursuit deux finalités différentes, cela implique que d'une part, les accès et la gestion du système de recherche soient gérés par les agents de la CSSF habilités spécialement à cet effet (département de sécurité informatique par exemple) et d'autre part, les recherches de données sur ce système soit effectuées par ses agents habilités en matière de lutte contre le blanchiment d'argent et le financement du terrorisme.

VIII. Quant à la publication des décisions de sanctions de la CSSF

70. La CNPD accueille avec intérêt les dispositions de l'article 5, paragraphe 6 de la loi modifiée du 25 mars 2020 qui prévoient un certain nombre de garanties lorsqu'une décision de sanction par la CSSF contenant des données personnelles est publiée. La loi modifiée du 25 mars 2020 prévoit en effet l'évaluation au cas par cas, par la CSSF, du caractère proportionné de la publication de l'identité des personnes responsables, le recours à l'anonymisation si elle garantit effectivement la protection des données à caractère personnel et une durée maximale de conservation de douze mois des données à caractère personnel dans la publication sur le site internet officiel de la CSSF.

IX. Quant aux dispositions relatives à la mise en place d'un registre des prestataires de services d'actifs virtuels



71. L'article 11 de la loi modifiée du 25 mars 2020 introduit l'article 7-1 modifiant la loi modifiée du 12 novembre 2004 et prévoyant la mise en place d'un registre des prestataires de services d'actifs virtuels par la CSSF.
72. Il ressort du dernier alinéa de l'article 7-1 (2) que la CSSF tient et met à jour le registre et le publie sur son site internet. Or, cette même disposition prévoit que dans le cas d'une personne physique requérante, ses nom et prénom(s), son adresse privée précise ou son adresse professionnelle précise et son numéro d'identification (national ou étranger) doivent être indiqués dans la demande d'enregistrement²³. Si le registre public reprenait les données fournies dans la demande d'enregistrement, et aucune justification n'étant avancée dans le commentaire des articles, la CNPD s'interroge sur la nécessité de publier ces données personnelles.
73. En effet, l'article 5, paragraphe 1^{er}, lettre (c) du RGPD prescrit que seules les données adéquates, pertinentes et nécessaires au regard des finalités poursuivies par le responsable du traitement doivent être traitées. Par ailleurs, selon l'article 25, paragraphe 2 du RGPD, le responsable du traitement doit « *mettre en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées* » (protection des données par défaut). Il importe ainsi de limiter au strict nécessaire les informations disponibles au public dès la conception du traitement.
74. Au vu de ce qui précède, la CNPD estime dès lors nécessaire de ne pas mentionner l'adresse privée précise et le numéro d'identification dans la liste des informations publiées sur le site internet de la CSSF²⁴.
75. L'article 7-1, paragraphes 3 et 3bis²⁵ prévoient par ailleurs que l'enregistrement dans un tel registre est subordonné à la condition que les personnes qui exercent une fonction de direction au sein de ces entités et les bénéficiaires effectifs desdites entités (qui peuvent être des personnes physiques) ou les personnes physiques qui exercent l'activité de prestataire de

²³ Tel que cela ressort de l'article 7 introduit par la loi du 25 février 2021 portant modification de :
1° la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme ;
2° la loi modifiée du 20 avril 1977 relative à l'exploitation des jeux de hasard et des paris relatifs aux épreuves sportives ;
3° la loi modifiée du 17 décembre 2010 concernant les organismes de placement collectif ;
4° la loi du 25 mars 2020 instituant un système électronique central de recherche de données concernant des comptes IBAN et des coffres-forts ;
5° la loi du 10 juillet 2020 instituant un Registre des fiducies et des trusts.

²⁴ Cf. arrêt de la CJUE du 22 novembre 2022, WM et Sovim SA, affaires jointes C 37/20 et C 601/20

²⁵ Paragraphe (3bis) introduit par la loi du 25 février 2021 portant modification de :
1° la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme ;
2° la loi modifiée du 20 avril 1977 relative à l'exploitation des jeux de hasard et des paris relatifs aux épreuves sportives ;
3° la loi modifiée du 17 décembre 2010 concernant les organismes de placement collectif ;
4° la loi du 25 mars 2020 instituant un système électronique central de recherche de données concernant des comptes IBAN et des coffres-forts ;
5° la loi du 10 juillet 2020 instituant un Registre des fiducies et des trusts.

services d'actifs virtuels adressent à la CSSF les informations nécessaires pour justifier de leur honorabilité professionnelle.

76. Or, la CNPD se demande quels sont les critères d'appréciation d'une telle « honorabilité » alors qu'aucune précision supplémentaire n'est indiquée dans la loi modifiée du 25 mars 2020. De même qu'elle se demande quelles sont les « informations nécessaires » pour justifier de l'honorabilité professionnelle. L'article 11, paragraphe 3, précise uniquement que « *l'honorabilité s'apprécie sur base de antécédents judiciaires et de tous les éléments susceptibles d'établir que les personnes visées à l'alinéa 1^{er} jouissent d'une bonne réputation et présentent toutes les garanties d'une activité irréprochable* ». De telles notions dont celle d'« antécédents judiciaires » ne sont pas détaillées dans la loi sous avis. D'après le commentaire des articles, la loi modifiée du 25 mars 2020 reprend la formulation de l'article 13 de la loi du 10 novembre 2009 relative aux services de paiement mais cette dernière ne précise pas davantage ces notions.
77. Concernant la notion d'« honorabilité », il convient d'attirer l'attention des auteurs de la loi sur le fait qu'une notion similaire est présente dans la loi modifiée du 2 septembre 2011 réglementant l'accès aux professions d'artisan, de commerçant, d'industriel ainsi qu'à certaines professions libérales (ci-après, la « loi modifiée du 2 septembre 2011 »), le règlement grand-ducal du 1^{er} décembre 2011 déterminant les modalités de l'instruction administrative prévue à l'article 28 de la loi modifiée du 2 septembre 2011 (ci-après, le « règlement grand-ducal du 1^{er} décembre 2011 »).
78. Par exemple, le chapitre 3 de la loi modifiée du 2 septembre 2011 intitulé « L'honorabilité professionnelle » définit cette notion et en précise les critères d'appréciation. L'article 2, paragraphe (4) du règlement grand-ducal du 1^{er} décembre 2011 précise quant à lui les pièces devant être fournies par le demandeur et sur lesquelles son honorabilité sera appréciée.
79. La CNPD estime dès lors nécessaire que les critères d'appréciation de l'honorabilité telle que visée à l'article 11, paragraphe 3, soient précisés. Les auteurs de la loi pourraient s'ils le souhaitent s'inspirer des dispositions légales précitées concernant la délivrance d'une autorisation d'établissement.
80. En tout état de cause, la Commission nationale regrette que le législateur adopte une approche sectorielle et non une approche globale et transversale de la question de l'appréciation de l'honorabilité. A cet égard, la CNPD renvoie à ses développements dans son avis relatif au projet de loi n°7989²⁶.
81. Par ailleurs, il ressort de la dernière partie du paragraphe 3 de l'article 7-1 que « *la CSSF peut demander tous renseignements nécessaires sur les personnes susceptibles de devoir remplir les*

²⁶ Voir Avis de la Commission nationale pour la protection des données relatif au projet de loi n°7989 portant modification 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 et au projet de règlement grand-ducal ayant pour objet de déterminer la composition et le fonctionnement de la commission de la seconde chance et portant modification de certains autres règlement grand-ducaux, Délibération n° 30/AV17/2023 du 7 avril 2023

conditions légales d'honorabilité ou d'expérience professionnelles ». La CNPD regrette que cet article ne mentionne pas à qui la CSSF peut demander ces renseignements.

X. Quant aux dispositions relatives à la mise en place d'une liste prestataires de services aux sociétés et fiduciaires

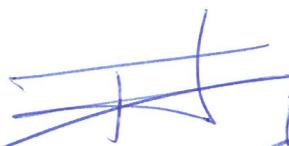
82. L'article 7-2, paragraphe 3 de la loi modifiée du 12 novembre 2004 prévoit quant à lui l'établissement par les autorités de contrôle et les organismes d'autorégulation d'une liste des prestataires de services aux sociétés et fiduciaires pour lesquels ils sont compétents. Le commentaire des articles précise que la finalité d'une telle liste est de faciliter la coordination entre les autorités de contrôle et les organismes d'autorégulation (dans le cadre de la lutte contre le blanchiment d'argent et le financement du terrorisme).
83. La Commission nationale déplore que les finalités de l'établissement de cette liste ne soient pas plus clairement exposées dans la loi modifiée du 25 mars 2020. Par ailleurs, il n'est pas non plus précisé si une telle liste reprendrait toutes les données communiquées lors de la demande d'enregistrement conformément à l'article 7-2, paragraphe 1, si l'accès en serait limité aux autorités de contrôle et aux organismes d'autorégulation et quelle(s) entité(s) serai(en)t responsable(s) du traitement d'une telle liste. La CNPD estime dès lors nécessaire de préciser la loi modifiée du 25 mars 2020 sur ces aspects.

Ainsi adopté à Belvaux en date du 9 juin 2023.

La Commission nationale pour la protection des données



Tine A. Larsen
Présidente



Thierry Lallemand
Commissaire



Alain Herrmann
Commissaire



Marc Lemmer
Commissaire