Le Règlement Général sur la Protection des Données

Lignes directrices en matière de durées de conservation des données personnelles par les prestataires de services de paiement

Date de la première adoption : 06/06/2025

Table des matières

Introduction

1. Ces lignes directrices s'adressent principalement aux prestataires de services de paiement (ci-après les « PSP » ou « responsables du traitement ») au sens de la loi modifiée du 10 novembre 2009 relative aux services de paiement[1] (ci-après la « Loi de 2009 »)[2].

2. Les prestataires de service de paiement collectent et traitent un volume important de données personnelles, au moment de l'entrée en relation, pendant toute la durée de la relation, et même bien après la fin de la relation avec l'utilisateur du service (ci-après l'« utilisateur » ou la « personne concernée »). Par ailleurs, les innovations technologiques ont fortement accru la capacité des prestataires de services de paiement à recueillir, stocker, combiner et analyser un large éventail de données concernant leurs utilisateurs.

3. Les données à caractère personnel susceptibles d'être traitées par des PSP peuvent comprendre des informations sur la situation personnelle de la personne concernée (âge, nationalité, situation matrimoniale…), sa situation économique et financière, les données de paiement (telles que le montant de la transaction, la date et l'heure du paiement, l'identité du bénéficiaire d'une transaction, l'IBAN ou encore les données de sécurité personnalisées), le score de lutte anti-fraude de la personne concernée, les données contextuelles ou comportementales (préférences et habitudes de consommation, géolocalisation, caractéristiques du terminal utilisé pour un achat en ligne, temps passé à prospecter…).

4. Or, bien qu'elles ne bénéficient pas d'un statut particulier en vertu du règlement général sur la protection des données (UE) 2016/679 (ci-après le « RGPD »), nombre de ces données sont à considérer comme des données « sensibles » (au sens commun du terme) dans la mesure où leur violation pourrait avoir des incidences graves dans la vie quotidienne de la personne concernée[3].

5. Eu égard l'ampleur de ces traitements, la CNPD souhaite rappeler certains des principes clés de l'article 5 du RGPD en ce qui concerne le traitement des données des utilisateurs des services de paiement. Un PSP ne peut traiter les données à caractère personnel d'une personne concernée que si le traitement envisagé est **licite**; c'est-à-dire nécessaire à l'exécution du contrat avec l'utilisateur, nécessaire au respect d'une obligation légale à laquelle le PSP est soumis, nécessaire aux fins des intérêts légitimes poursuivis par le PSP ou, dans des cas plus rares, sur l'une des autres bases juridiques pour le traitement des données mentionnées à l'article 6 du RGPD. Conformément au principe de **transparence**, les personnes concernées doivent conserver la maîtrise des données qui les concernent. Cela suppose qu'elles soient clairement informées de l'utilisation qui sera

[1] https://www.cssf.lu/fr/Document/loi-du-10-novembre-2009/

[2] Si les principes exposés dans les présentes lignes directrices peuvent également s'appliquer à d'autres professionnels du secteur financier, la présente guidance n'a cependant pas pour objet d'exposer les spécificités applicables pour les autres professionnels.

[3] Lignes directrices du groupe de travail «Article 29» concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679, WP248 rev.01 – approuvées par l'EDPB (p.11) ; Lignes directrices 6/2020 relatives à l'interaction entre la deuxième directive sur les services de paiement et le RGPD, Version 2.0, Adoptées le 15 décembre 2020 (§69).

faite de leurs données dès leur collecte et tout au long du cycle de vie du traitement. De plus, les données personnelles des utilisateurs ne peuvent être traitées que pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités (principe de **limitation des finalités**). Les données doivent également être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (principe de **minimisation des données**). Elles doivent aussi être exactes et, si nécessaire, tenues à jour (principe d'**exactitude**).

6. Enfin, selon l'article 5.1 (e) du RGPD, les données à caractère personnel doivent être « *conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées* […] » (principe de **limitation de la conservation des données**). Les présentes lignes directrices n'aborderont pas en détails la question des données nécessaires à l'exécution des contrats qui sont conservées pendant la durée de la relation contractuelle mais plutôt l'ensemble des aspects relatifs aux durées de conservation une fois cette relation avec la personne concernée terminée. En effet, les PSP conservent généralement les données personnelles de leurs utilisateurs afin de respecter certaines obligations légales ou afin de se prémunir de certaines actions en justice pendant les durées de prescriptions légales.

7. Sans prétendre à l'exhaustivité, ces lignes directrices ont pour objectif d'éclairer les acteurs concernés sur les durées et modalités de conservation des données personnelles qu'ils traitent dans le contexte d'un secteur fortement régulé. La protection des données à caractère personnel est de plus en plus ancrée dans les différentes réglementations européennes (également celles applicables spécifiquement au secteur financier) et la CNPD souhaiterait éclairer autant que possible les responsables du traitement concernés sur l'application de certaines de ces dispositions par rapport aux exigences du RGPD en matière de durées de conservation des données personnelles. Avec la présence de nombreux prestataires de services de paiement agissant en tant que responsables du traitement basés au Luxembourg[4] et conformément aux recommandations du Comité européen de la protection des données (ci-après le « CEPD ») et du législateur européen, la CNPD entend en effet adopter une approche holistique du cadre réglementaire applicable aux acteurs du secteur financier, et ce en coopération avec les autres autorités compétentes au Luxembourg[5][6].

[4] En mai 2025, on dénombre au Luxembourg 117 établissements de crédit, 17 établissements de paiement et 12 établissements de monnaie électronique (source : https://www.cssf.lu/wp-content/uploads/newsletter282.pdf)

[5] Cf. *EDPB Strategy 2024-2027* : « *L'EDPB s'emploiera à renforcer la coopération avec d'autres autorités de régulation, en vue d'intégrer le droit à la protection des données dans l'architecture réglementaire globale*. »

[6] Cf. considérant 130 de la Proposition de Règlement concernant les services de paiement dans le marché intérieur et modifiant le règlement (UE) nº 1093/2010, 28.06.2023 (2023/0210 (COD)): « *L'efficacité du cadre de l'Union relatif aux services de paiement dépend de la coopération entre de multiples autorités compétentes, notamment des autorités nationales chargées de la fiscalité, de la protection des données, de la concurrence, de la protection des consommateurs, de l'audit, de la police et d'autres autorités chargées de faire respecter la législation. Les États membres devraient veiller à ce que leur cadre juridique permette et facilite cette coopération en tant que de besoin pour atteindre*

1. Le principe de limitation de la conservation

8. Conformément à l'article 5.1 (e) du RGPD, les données à caractère personnel « *doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées.* ».

   Il ressort par ailleurs du considérant 39 du RGPD que « *les données à caractère personnel devraient être adéquates, pertinentes et limitées à ce qui est nécessaire pour les finalités pour lesquelles elles sont traitées. Cela exige, notamment, de garantir que la durée de conservation des données soit limitée au strict minimum. Les données à caractère personnel ne devraient être traitées que si la finalité du traitement ne peut être raisonnablement atteinte par d'autres moyens. Afin de garantir que les données ne sont pas conservées plus longtemps que nécessaire, des délais devraient être fixés par le responsable du traitement pour leur effacement ou pour un examen périodique. Il y a lieu de prendre toutes les mesures raisonnables afin de garantir que les données à caractère personnel qui sont inexactes sont rectifiées ou supprimées.* ».

9. Concernant le caractère adéquat, pertinent et limité de ce qui est nécessaire pour les finalités du traitement, il y a lieu de rappeler les précisions apportées par le CEPD concernant la précision des finalités des traitements entrepris par un responsable du traitement :

   « 40. Un responsable du traitement doit déterminer la base juridique appropriée pour les traitements envisagés avant de procéder au traitement des données. ***Lorsque l'article 6, paragraphe 1, point b), constitue la base de tout ou partie des activités de traitement, le responsable du traitement devrait anticiper ce qui se passera en cas de résiliation du contrat****.*

   [...]

   43. L'article 17, paragraphe 1, point a), dispose que les données à caractère personnel sont effacées lorsqu'elles ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées. Cette règle ne s'applique toutefois pas si le traitement est nécessaire pour certaines finalités spécifiques, notamment le respect d'une obligation légale en vertu de l'article 17, paragraphe 3, point b), ou la constatation, l'exercice ou la défense de droits en justice en vertu de l'article 17, paragraphe 3, point e). Dans la pratique, ***si les responsables du traitement constatent un besoin général de conserver des registres à des fins légales, ils doivent déterminer une base juridique pour cette conservation dès le début du traitement, et doivent communiquer clairement, au même moment, la durée pendant laquelle ils prévoient de conserver les registres à ces fins légales après la résiliation du contrat****. Dans ce cas, ils ne sont pas obligés d'effacer les données après la résiliation du contrat.*

   44. En tout état de cause, ***il est possible que plusieurs traitements présentant des finalités et des bases juridiques distinctes aient été identifiés dès le début du traitement.*** *Tant que ces autres traitements restent licites et que le responsable du*

---

les objectifs du cadre de l'Union relatif aux services de paiement, y compris par la bonne application de ses règles. […]»

traitement a communiqué clairement ces opérations au début du traitement, conformément aux obligations de transparence du RGPD, il sera toujours possible de traiter des données à caractère personnel concernant la personne concernée pour ces finalités distinctes après la résiliation du contrat."[7]

10. Une fois la ou les finalité(s) du traitement atteinte(s), la conservation de certaines données pour le respect d'obligations légales ou à des fins précontentieuses ou contentieuses est donc possible, mais les données doivent alors être archivées, pour une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont conservées, conformément aux dispositions en vigueur.

11. Dans le contexte d'une relation contractuelle entre la personne concernée et un prestataire de services de paiement, il convient de distinguer deux phases dans le cycle de vie des données personnelles de l'utilisateur:

    (i) **La phase active** : la conservation des données personnelles du client pendant la durée de la relation contractuelle, principalement sur base de la nécessité du traitement à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci (article 6.1 (b) du RGPD), de la nécessité au respect d'une obligation légale (article 6.1 (c) du RGPD) ou, plus exceptionnellement, sur une autre base légale prévue à l'article 6 du RGPD, comme le consentement de la personne concernée (article 6.1 (a) du RGPD) ou l'intérêt légitime du responsable du traitement (article 6.1 (f) du RGPD) (on parlera ici de phase d' « utilisation courante » des données personnelles) ;

    (ii) **La phase d'archivage** : la conservation ou « archivage » des données personnelles du client après la fin de la relation contractuelle (correspondant en pratique avec la clôture du compte de l'utilisateur), le plus souvent sur base de la nécessité au respect d'une obligation légale (article 6.1 (c) du RGPD) ou, plus exceptionnellement, sur une autre base légale prévue à l'article 6 du RGPD (par exemple l'intérêt légitime du responsable du traitement, prévu à l'article 6.1 (f) du RGPD).

12. Quand la durée de conservation dans le cadre de l'archivage est dépassée, le responsable du traitement doit procéder à l'effacement des données à caractère personnel (qui est un droit pour la personne concernée conformément à l'article 17 du RGPD). Il peut, par exemple, les détruire de manière définitive ou bien les anonymiser.

Les présentes lignes directrices se focalisent sur l'application du principe de limitation de conservation des données dans le cadre de l'archivage. A chaque fois qu'il sera fait référence à une durée de conservation dans ce document, il s'agira de la 2eme phase du cycle de vie de la donnée, c'est-à-dire la phase d'archivage suite à la clôture du compte d'un client).

[7] CEPD, Lignes directrices 2/2019 sur le traitement des données à caractère personnel au titre de l'article 6, paragraphe 1, point b), du RGPD dans le cadre de la fourniture de services en ligne aux personnes concernées, Version 2.0, Adoptées le 8 octobre 2019

13. Conformément au principe de responsabilité énoncé à l'article 5.2 du RGPD, tout responsable du traitement doit être en mesure de démontrer que l'ensemble des principes de l'article 5.1 du RGPD sont respectés (y compris le principe de minimisation des données de l'article 5.1 (c) et le principe de limitation de la conservation de l'article 5.1 (e)). Pour cela, le responsable du traitement devra 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 soient traitées dans le cadre de la période de conservation (article 25.2 d RGPD). A cette fin, le responsable du traitement de données devra définir précisément le point de départ de chaque durée de conservation afin de pouvoir automatiquement respecter cette obligation sans attendre une demande d'effacement de la part de la personne concernée.

14. Afin de définir de la manière la plus précise possible la durée de conservation de chaque ensemble de données personnelles qu'il traite et le point de départ de cette durée, le responsable du traitement doit :
    - définir précisément les finalités poursuivies (il n'est pas possible de conserver les données « au cas où … ») ainsi que les bases de licéité applicables, et
    - déterminer, en fonction de chaque finalité spécifique, une durée de conservation appropriée et nécessaire afin d'atteindre ladite finalité.

15. Si les données sont utilisées dans plusieurs traitements poursuivant plusieurs finalités, les durées de conservation sont à individualiser pour chaque finalité spécifique.

A retenir : Le responsable du traitement doit définir la durée de conservation ou les modalités pour calculer la durée de conservation **pour chaque traitement de données**.

L'absence de spécification de durée de conservation ou une durée de conservation illimitée constitue une violation du RGPD. Une même donnée personnelle peut être utilisée pour des traitements distincts et peut donc être nécessaire pendant des durées différentes. La fin d'un traitement de données pour lequel une donnée a été utilisée n'implique donc pas que la donnée doit être effacée, si elle reste toujours nécessaire pour un autre traitement de données en cours.

Dans un tel cas de figure, il est nécessaire de bien distinguer les différentes activités de traitement de données et de leur appliquer à chacune une durée pertinente par rapport à leurs finalités respectives. Ainsi, les données associées à la durée la plus longue seront conservées et ne seront pas supprimées à la fin du premier traitement.

Exemple 1 : Dans le cadre de sa relation contractuelle avec une personne concernée, un prestataire de services de paiement conserve son numéro de téléphone pour des finalités d'authentification ou de communication avec cette dernière dans le cadre de son contrat. Une fois le contrat résilié, le traitement de cette donnée n'est plus nécessaire à l'exécution du contrat et le prestataire de service de paiement devra procéder à son effacement (à moins qu'il ne démontre que le traitement du numéro de téléphone de l'utilisateur est nécessaire pour certaines finalités spécifiques, notamment le respect d'une obligation légale en vertu de l'article 17.3, point b), ou la constatation, l'exercice ou la défense de droits en justice en vertu de l'article 17.3, point e).

Exemple 2 : Un prestataire de services de paiement traite également l'adresse postale de la résidence principale de la personne concernée. Cette donnée est traitée pour différentes finalités liées à la gestion de la relation avec le client mais également dans le cadre des obligations de vigilance du prestataire de services de paiement prévues par la loi du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme, telle que modifiée (la « Loi de 2004 »). Or, l'article 3.6 de cette loi prévoit une obligation de conservation des données collectées dans le cadre des mesures de vigilance à l'égard du client pendant cinq ans après la fin de la relation d'affaires avec le client ou après la date de la transaction conclue à titre occasionnel. Il conviendra donc de retenir la durée de conservation la plus longue et il ne sera pas nécessaire d'effacer l'adresse de la personne concernée lors de la résiliation du contrat (date à laquelle certaines finalités du traitement de l'adresse disparaissent) mais bien cinq ans après la fin du contrat.

2. Définition de la base de licéité pour la conservation et de la durée de conservation

a. Article 6.1 (c) RGPD : conservation nécessaire au respect d'une obligation légale

L'article 6.1. (c) du RGPD prévoit la licéité d'un traitement si ce traitement "*est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis*". De manière générale, les durées de conservation ne devraient, en principe, pas dépasser les durées de prescription légales.

i. Durée de conservation décennale (Code de commerce)

16. L'article 16 du Code de commerce prévoit l'obligation pour les commerçants de conserver les documents ou informations visés aux articles 11, 12, 14 et 15 « *pendant dix ans à partir de la clôture de l'exercice auquel ils se rapportent* », mais uniquement pour des finalités de comptabilité. Dès lors, toutes les données personnelles d'un client traitées dans le cadre de la comptabilité (registres, livres et pièces comptables), les lettres reçues et les copies des lettres envoyées peuvent donc être conservées par le responsable du traitement pour une durée de 10 ans à partir de la clôture de l'exercice auquel ils se rapportent (ce qui coïncide en général avec la fin de l'année civile). Les données personnelles conservées sur base de cette disposition doivent donc faire l'objet d'un effacement à intervalle régulier, sauf si elles sont également traitées pour une autre finalité (par ex. le respect d'une autre obligation légale prévoyant une durée de conservation plus longue). Une donnée personnelle collectée dans le cadre de l'exercice comptable de l'année 2024 devra donc être effacée ou anonymisée par le responsable du traitement au 1er janvier 2035, même si le compte de la personne concernée n'a toujours pas été clôturé.

Exemple 3 : L'arrêté de compte du client d'une banque pourra être conservé pendant 10 ans après la fermeture de son compte. En revanche, la copie de sa carte d'identité qui a été collectée dans le cadre des obligations de la banque issues de la Loi de 2004, et qui n'est pas traitée par la banque dans le cadre de sa comptabilité, devra être effacée cinq ans après la fermeture du compte du client (à moins que la banque ne soit en mesure de démontrer qu'une période de conservation prolongée de cinq ans supplémentaires est nécessaire pour la mise en œuvre efficace des mesures internes de prévention ou de détection des actes de blanchiment de capitaux ou de financement du terrorisme conformément à l'article 3.6 de la loi précitée).

17. Par ailleurs, l'article 27 (intitulé « L'archivage ») de la Loi de 2009 impose aux établissements de paiement et aux établissements de monnaie électronique de « *conserver, conformément aux délais prévus au Code de commerce, tous les enregistrements appropriés pour permettre à la CSSF de contrôler qu'ils respectent les obligations qui leur incombent en vertu de la présente loi* ».

18. De plus, si on se réfère à la loi du 5 avril 1993 relative au secteur financier telle qu'elle a été modifiée, les établissements de crédit doivent prévoir l'enregistrement et la conservation, conformément aux délais prévus au Code de commerce, « *de tout service fourni, de toute activité exercée et de toute transaction effectuée par eux-mêmes* » (article 37-1 (paragraphe 6)). Les données collectées et conservées sur base des dispositions nationales précitées peuvent donc en principe être conservées pendant maximum 10 ans **à partir de la clôture de l'exercice auquel elles se rapportent** et puis être effacées ou anonymisées par le responsable du traitement (sauf autre durée de conservation plus longue applicable à ces données).

ii. Durée de conservation des données pour la finalité de la lutte contre le blanchiment et le financement du terrorisme (Loi 2004)

19. Conformément à l'article 3.6 de la Loi de 2004, à l'article 1.5 du Règlement grand-ducal du 1er février 2010 portant précision de certaines dispositions de la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme et à l'article 25 du Règlement CSSF N° 12-02 du 14 décembre 2012 relatif à la lutte contre le blanchiment et contre le financement du terrorisme, tel que modifié (ci-après « le Règlement CSSF »), les professionnels sont tenus de conserver pendant cinq ans après la fin de la relation d'affaires avec le client ou après la date de la transaction conclue à titre occasionnel les documents, données et informations suivantes:
    - une copie des documents, des données et informations qui sont nécessaires pour se conformer aux obligations de vigilance à l'égard de la clientèle prévues aux articles 3 à 3-3 de la Loi de 2004, les livres de comptes, la correspondance commerciale, ainsi que les résultats de toute analyse réalisée,
    - les pièces justificatives et enregistrements de transactions qui sont nécessaires pour identifier ou reconstituer des transactions individuelles afin de fournir, si nécessaire, des preuves dans le cadre d'une enquête ou instruction pénale.

20. La CNPD relève que les données personnelles conservées sont par exemple celles contenues dans des documents officiels d'identification des clients tels que les passeports, les cartes d'identité, les permis de conduire ou d'autres documents similaires ou les copies de ces documents ; les recherches visant à établir le contexte et l'objet des opérations complexes d'un montant anormalement élevé ; les données relatives aux bénéficiaires effectifs (par exemple celles extraites depuis le registre des bénéficiaires effectifs), etc.

21. La CNPD note également que la conservation de certaines données sur base des dispositions précitées peut, dans des cas plus rares, également porter sur des catégories particulières de données à caractère personnel au sens de l'article 9 du RGPD ou des données à caractère personnel relatives aux condamnations pénales et aux infractions au sens de l'article 10 du RGPD[8].

[8] Conseil de l'Europe, Comité consultatif de la convention pour la protection des personnes à l'égard du traitement des données à caractère personnel, Convention 108, Lignes directrices sur la protection des données personnelles dans le traitement des données personnelles en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme (p.20)

22. En effet, les opinions politiques et les croyances religieuses peuvent être révélées par les opérations financières, par exemple, par des dons faits à des partis politiques ou à des organisations, à des églises ou à des paroisses. L'appartenance à un syndicat peut être révélée par le prélèvement d'une cotisation annuelle sur le compte bancaire d'une personne. Des données à caractère personnel concernant la santé peuvent être obtenues en analysant les factures médicales payées par une personne concernée à un professionnel de la santé (par exemple, un psychiatre). Enfin, des informations sur certains achats peuvent révéler des informations sur la vie sexuelle ou l'orientation sexuelle d'une personne[9].

23. Par ailleurs, les obligations de vigilance découlant de la Loi de 2004 pourraient amener les responsables du traitement à collecter et conserver des données concernant une procédure judiciaire menée contre une personne physique, telles que celles relatant sa mise en examen ou le procès, et, le cas échéant, la condamnation qui en a résulté, qui constituent des données relatives aux « infractions » et aux « condamnations pénales », au sens de l'article 10 du RGPD, et ce indépendamment du fait que, au cours de cette procédure judiciaire, la commission de l'infraction pour laquelle la personne était poursuivie a effectivement été établie ou non[10].

24. Etant donné que le contexte dans lequel ce type de données sont traitées pourrait engendrer des risques importants pour les libertés et droits fondamentaux des personnes concernées[11], les traitements de données couvertes par les articles 9 et 10 du RGPD impliquent pour le responsable du traitement la mise en place d'un certain nombre de garanties supplémentaires, comme par exemple une information spécifique que ces catégories de données sont susceptibles d'être traitées aux fins du respect de la Loi de 2004 ou encore un mécanisme permettant au responsable du traitement de s'assurer que les données proviennent de sources fiables, sont exactes et à jour[12].

25. Les entités soumises à la Loi de 2004 peuvent conserver les données personnelles de leurs clients pour une période supplémentaire de cinq ans « *lorsque cette conservation est nécessaire pour la mise en œuvre efficace des mesures internes de prévention ou de détection des actes de blanchiment de capitaux ou de financement du terrorisme*. » (article 3.6, alinéa 6) ou lorsqu'une période de conservation supplémentaire est exigée par les autorités de contrôle (article 3.6, alinéa 5). Conformément à cette disposition, la CNPD rappelle qu'une durée de 10 ans ne devrait pas être la durée de conservation « par défaut » pour tous les clients d'un prestataire de service de paiement. Il appartient au

---

[9] CEPD, Lignes directrices 6/2020 relatives à l'interaction entre la deuxième directive sur les services de paiement et le RGPD, Version 2.0, adoptées le 15 décembre 2020 (§52) ; Contrôleur européen de la protection des données, Avis 39/2023 sur la proposition de règlement concernant les services de paiement, dans le marché intérieur et la proposition de directive concernant les services de paiement et les services de monnaie électronique dans le marché intérieur, adopté le 22 août 2023 (§24).

[10] Arrêt du 24 septembre 2019, GC e.a. (Déréférencement de données sensibles), C-136/17, EU:C:2019:773, point 72.

[11] Cf. considérant (51) du RGPD.

[12] La CNPD invite les responsables du traitement à prendre connaissance de l'article 76 du Règlement 2024/1624 du 31 mai 2024 relatif à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme qui prévoit les conditions du traitement des données visées aux articles 9 et 10 du RGPD (bien que cette disposition ne soit pas encore applicable, celle-ci pourrait déjà servir de « standard » pour les professionnels concernés).

responsable du traitement, conformément au principe de responsabilité, de documenter pourquoi les motifs pour lesquels une période supplémentaire de cinq ans est nécessaire.

26. Il est également important de noter que la Loi de 2004 prévoit que « *[s]ans préjudice des délais de conservation plus longs prescrits par d'autres lois, les professionnels sont tenus d'effacer les données à caractère personnel à l'issue des périodes de conservation visées à l'alinéa 1er*. » (article 3.6, alinéa 4). L'obligation d'effacer les données des personnes concernées après 5 ou 10 ans (après la fin de la relation d'affaires avec le client ou après la date de la transaction conclue à titre occasionnel) ressort donc également de la loi de 2004. Il en ressort que les responsables du traitement ne devraient donc pas conserver les données au-delà de ces délais pour des finalités de lutte contre le blanchiment et de financement de terrorisme.

A retenir : Lorsqu'une obligation légale impose au responsable du traitement d'effacer les données, il ne peut pas conserver les données collectées pour le respect de cette obligation légale au-delà du délai de conservation légale sur base de son intérêt légitime.

27. La CNPD prend également note de l'article 11.2 du Règlement CSSF, tel que modifié, selon lequel : « *La politique d'acceptation des clients doit également prévoir les procédures à suivre lors d'un soupçon ou de motifs raisonnables de soupçon de blanchiment, d'une infraction sous-jacente associée ou de financement du terrorisme en cas de non-aboutissement d'une entrée en contact avec un client potentiel. Les raisons d'un refus de la part du client ou du professionnel de nouer une relation d'affaires ou d'effectuer une transaction doivent être documentées et conservées selon les modalités prévues à l'article 25 du présent règlement, et ce, même si le refus de la part du professionnel ne découle pas de la constatation d'un indice de blanchiment ou de financement du terrorisme.* ». Par conséquent, les données d'une personne concernée qui se voit refuser l'ouverture d'un compte ou renonce elle-même à cette ouverture pourront être conservées selon les règles prévues par la Loi de 2004.

28. Au vu de ce qui précède, la CNPD distingue principalement trois points de départ possibles pour le calcul des durées de conservation prescrites par l'article 3.6 de la Loi de 2004 :
    (i) la fin de la relation d'affaire avec le client (ce qui correspond par exemple à la fermeture du compte bancaire ou compte en ligne d'une personne concernée) ;
    (ii) la date d'une transaction conclue à titre occasionnelle ;
    (iii) la date du refus d'entrée en relation d'affaire par le client ou le professionnel.

29. La CNPD constate qu'il peut arriver qu'un compte soit bloqué par le responsable du traitement pour des raisons tenant à l'application de la Loi de 2004 (par exemple, conformément à l'article 3.4 de la Loi de 2004 dans l'attente d'une vérification d'identité) et qu'en cas d'absence de réaction de la part du client, le compte reste indéfiniment bloqué et ne permet pas de déclencher une durée de conservation. Cette situation pouvant conduire dans certains cas à une conservation des données de la personne concernée pour une durée illimitée en violation de l'article 5.1 (e) du RGPD[13], la CNPD recommande aux responsables du traitement concernés de mettre en place un mécanisme permettant de relancer la personne concernée et de procéder à la clôture du compte au plus tard un an après le blocage du compte (les données personnelles étant de toute façon conservées suite à la clôture pour des finalités de lutte contre le blanchiment et le terrorisme).

[13] Et des exigences de l'article 3.4 de la Loi de 2004.

iii. Durées de conservation spéciales pour la finalité de la lutte contre le blanchiment et le financement du terrorisme (Régl. UE 2023/1113)

30. L'article 26.1 du Règlement (UE) du Parlement et du Conseil 2023/1113 du 31 mai 2023 sur les informations accompagnant les transferts de fonds et de certains crypto-actifs, et modifiant la directive (UE) 2015/849 rappelle que les informations sur le donneur d'ordre et le bénéficiaire de fonds ou sur l'initiateur et le bénéficiaire de crypto-actifs (telles que, entre autres, le nom, le numéro de compte de paiement, l'adresse, le numéro du document d'identité officiel, le numéro d'identification de client, la date et le lieu de naissance) ne sont pas conservées au-delà de ce qui est strictement nécessaire. Le prestataire de services de paiement doit ainsi conserver ces données pendant une durée de cinq ans, période à l'issue de laquelle il doit les effacer (comme le précise l'article 26.2), sauf dispositions contraires du droit national précisant dans quelles circonstances les prestataires de services de paiement peuvent ou doivent prolonger la période de conservation de ces données. Etant donné que les données à caractère personnel traitées par les prestataires de services de paiement sur base de ce règlement ne le sont qu'aux fins de la prévention du blanchiment de capitaux et du financement du terrorisme (article 25.2), la CNPD comprend que le point de départ de la période de conservation précitée est le même que celui pour les traitements prévus par la Loi de 2004 à savoir la fin de la relation d'affaires avec le client ou la date de la transaction conclue à titre occasionnel.

Exemple 4 : une banque en ligne traite le numéro du document d'identité officiel de son client conformément à l'article 26.1 du Règlement (UE) du Parlement et du Conseil 2023/1113 du 31 mai 2023 sur les informations accompagnant les transferts de fonds et de certains crypto-actifs, et modifiant la directive (UE) 2015/849 et aux dispositions de la Loi de 2004. Cette donnée devra être effacée 5 ans après la fermeture du compte de la personne concernée.

iv. Enregistrement des conversations téléphoniques et des communications électroniques

31. L'enregistrement des conversations téléphoniques et des communications électroniques n'est, en principe, possible que dans le respect de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques (ci-après la « Loi de 2005 ») et du RGPD.

32. Ainsi, conformément à l'article 4.3 (d) de la Loi de 2005, les communications peuvent être enregistrées :
    - sur base du consentement préalable, libre, spécifique, éclairé et univoque du client ; ou

- lorsqu'il est effectué dans le cadre des usages professionnels licites, afin de fournir la preuve d'une transaction commerciale ou de toute autre communication commerciale.

33. L'exception des « *communications commerciales* » peut viser par exemple les enregistrements des conversations téléphoniques effectués par les « *call center* », les « *Help-desk* », les services après-vente, etc.

34. Dans les deux cas, il est nécessaire d'informer les clients et les salariés de manière préalable et transparente, notamment sur la ou les finalité(s) de l'enregistrement ainsi que la durée de conservation. Cette information doit répondre aux exigences du RGPD[14].

35. Pour respecter ces exigences, la CNPD estime nécessaire que lors de chaque entretien téléphonique soumis à surveillance, les correspondants soient spécifiquement rendus attentifs à l'enregistrement, moyennant diffusion d'un message automatisé ou non au début de l'appel.

36. En ce qui concerne plus spécifiquement les établissements de crédit, l'article 37-1 (paragraphe 6bis) de la loi du 5 avril 1993 relative au secteur financier telle qu'elle a été modifiée prévoit l'obligation de conserver les enregistrements des conversations téléphoniques ou des communications électroniques « *en rapport, au moins, avec les transactions conclues dans le cadre d'une négociation pour compte propre et la prestation de services relatifs aux ordres de clients qui concernent la réception, la transmission et l'exécution d'ordres de clients* **»** et ce « *pendant cinq ans et, lorsque la CSSF le demande, pendant une durée pouvant aller jusqu'à sept ans*. » Les conversations téléphoniques et communications électroniques doivent donc en principe être effacées cinq ans après leur enregistrement, à moins qu'une conservation plus longue ne soit justifiée par une autre finalité compatible avec la finalité initiale et qu'une des bases de licéité prévues à l'article 6 du RGPD ne soit applicable.

v. Collecte de la carte d'identité dans le cadre de l'exercice des droits des personnes concernées

37. Conformément à l'article 12.6 du RGPD, lorsque le responsable du traitement a des doutes raisonnables quant à l'identité de la personne physique présentant la demande visée aux articles 15 à 21 (par exemple, une demande d'accès ou d'effacement), il peut demander que lui soient fournies des informations supplémentaires nécessaires pour confirmer l'identité de la personne concernée.

38. De manière générale, la carte d'identité ne devrait pas être considérée comme un moyen d'authentification approprié pour confirmer l'identité de la personne concernée à moins qu'une évaluation de proportionnalité démontre le contraire. Une telle évaluation de proportionnalité doit tenir compte du type des données traitées, de la nature de la demande

[14] Cf. articles 12, 13 et 14 du RGPD. Pour plus d'informations, consulter le site internet de la CNPD, « le droit à l'information », disponible à l'adresse https://cnpd.public.lu/fr/particuliers/vos-droits/droit-a-information.html.

ainsi que du contexte de la demande tout en évitant une collecte excessive des données et en garantissant un niveau adéquat de sécurité du traitement[15].

39. Néanmoins, il peut arriver qu'un prestataire de services de paiement demande à une personne concernée souhaitant exercer ses droits prévus par le RGPD de fournir une copie de sa carte d'identité ou d'un autre document officiel prouvant son identité (lorsqu'une telle collecte est justifiée et proportionnée au titre du RGPD). Dans une telle situation, le responsable du traitement doit alors mettre en œuvre des garanties pour empêcher le traitement non autorisé ou illicite de la carte d'identité. Il peut s'agir notamment de s'abstenir de faire une copie après avoir vérifié la carte d'identité ou de supprimer une copie d'un document d'identité immédiatement après l'authentification réussie de l'identité de la personne concernée. Le CEPD a d'ailleurs rappelé que « *la conservation ultérieure d'une copie d'un document d'identité est susceptible de constituer une violation des principes de limitation des finalités et de limitation de la conservation [article 5, paragraphe 1, points b) et e) du RGPD] et, en outre, de la législation nationale relative au traitement du numéro d'identification national (article 87 du RGPD). L'EDPB recommande, à titre de bonne pratique, que le responsable du traitement, après avoir vérifié la carte d'identité, fasse une note, indiquant par exemple « la carte d'identité a été vérifiée » afin d'éviter la copie ou le stockage inutile de copies de cartes d'identité.* »[16].

40. La CNPD rappelle également que le traitement d'une carte d'identité à des fins d'authentification dans le contexte de l'exercice des droits des personnes concernées est sans préjudice des obligations de conservation d'une copie de la carte d'identité au titre de la Loi de 2004 (l'effacement de la carte d'identité collectée pour confirmer l'identité d'une personne exerçant par exemple un droit d'accès conformément à l'article 15 du RGPD, ne suppose pas l'effacement de sa carte d'identité conservée pour des finalités en lien avec la lutte contre le blanchiment et le financement du terrorisme (« LBC/FT ») dans une base de données à part)[17].

b. Article 6.1 (f) RGPD : conservation nécessaire aux fins des intérêts légitimes du responsable du traitement

i. Rappel des conditions du recours à l'intérêt légitime

41. L'article 6.1 (f) du RGPD prévoit la licéité d'un traitement si ce traitement « *est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant*. ».

[15] CEPD, Lignes directrices 01/2022 sur les droits des personnes concernées — Droit d'accès, Version 2.1, adoptées le 28 mars 2023, §§70-77.
[16] *Ibidem,* §79 et jurisprudence citée. CEPD, *Ibidem*, (§79 et jurisprudence citée)
[17] Cf. point 2.a.iii

42. La CNPD souhaite rappeler les trois conditions cumulatives pour qu'un responsable du traitement puisse se fonder sur l'article 6.1 (f) du RGPD[18] :
    i) la poursuite d'un intérêt légitime par le responsable du traitement ou par un tiers ;
    ii) la nécessité du traitement des données à caractère personnel pour la réalisation de l'intérêt légitime poursuivi (l'intérêt légitime du traitement des données poursuivi ne peut raisonnablement être atteint de manière aussi efficace par d'autres moyens moins attentatoires aux libertés et aux droits fondamentaux des personnes concernées) ;
    iii) les intérêts ou les libertés et les droits fondamentaux de la personne concernée par la protection des données ne prévalent pas sur l'intérêt légitime du responsable du traitement ou d'un tiers (c'est le cas par exemple lorsque des données personnelles sont traitées dans des circonstances où les personnes concernées ne s'attendent raisonnablement pas à un tel traitement).

43. Il convient d'interpréter les conditions de l'application de l'intérêt légitime de manière restrictive[19]. L'intérêt légitime ne doit pas constituer une base de licéité par défaut. La CNPD recommande de procéder à une mise en balance des droits et intérêts en cause pour chaque traitement, cette analyse devant être détaillée et documentée avant le traitement en cause.

44. Il s'agit ainsi d'évaluer le degré d'intrusion du traitement envisagé dans la sphère individuelle, en mesurant ses incidences sur la vie privée des personnes (traitement de données sensibles, traitement portant sur des personnes vulnérables, profilage, etc.) et sur leurs autres droits fondamentaux (liberté d'expression, liberté d'information, liberté de conscience, etc.) ainsi que les autres impacts concrets du traitement sur leur situation (suivi ou surveillance de leurs activités, exclusion bancaire, etc.). Ces incidences doivent être mesurées afin de déterminer, au cas par cas, l'ampleur de l'intrusion causée par le traitement dans la vie des personnes[20].

45. Le recours à cette base légale implique certaines obligations supplémentaires pour le responsable du traitement dans la gestion des droits des personnes concernées :
    - Obligation d'information spécifique concernant les intérêts légitimes poursuivis (article 13.1 (d) du RGPD lorsque les données personnelles sont collectées auprès de la personne concernée et 14.2 (b) du RGPD lorsque les données personnelles n'ont pas été collectées auprès de la personne concernée) ;
    - Droit d'opposition de la personne concernée (article 21.1 du RGPD) : droit de la personne concernée de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel la concernant fondé sur l'intérêt légitime, y compris un profilage fondé sur ces dispositions. Le responsable du traitement ne doit alors plus traiter les données personnelles, à moins qu'il ne démontre qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice ;
    - Droit à la limitation du traitement (article 18 du RGPD) : droit de la personne concernée d'obtenir la limitation d'un traitement lorsque la personne concernée s'est opposée au traitement en vertu de l'article 21.1 du RGPD, pendant la vérification portant sur le

[18] Arrêt du 4 juillet 2023, C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), point 106
[19] Arrêt du 4 juillet 2023, Meta Platforms e.a. (Conditions générales d'utilisation d'un réseau social), C-252/21, ECLI:EU:C:2023:537, points 92 et 93 et jurisprudence citée
[20] Arrêt du 4 juillet 2023, C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), points 116 et 118.

point de savoir si les motifs légitimes poursuivis par le responsable du traitement prévalent sur ceux de la personne concernée.

46. Pour plus de précisions sur les critères que les responsables du traitement doivent remplir pour traiter des données personnelles sur la base de l'intérêt légitime, la CNPD invite les acteurs concernés à prendre connaissance du projet de lignes directrices du CEPD sur l'intérêt légitime[21].

47. Dans les prochaines sections, la CNPD analysera des finalités qui pourraient être poursuivies sur base de l'intérêt légitime d'un prestataire de service de paiement.

ii. Conservation des données nécessaires à la constatation, à l'exercice ou à la défense de droits en justice

48. Le considérant 65 du RGPD précise que la conservation ultérieure des données à caractère personnel devrait être licite lorsqu'elle est nécessaire à la constatation, à l'exercice ou à la défense de droits en justice. Dans ce contexte, les durées de prescription peuvent donc donner des indications importantes pour déterminer les durées de conservation[22].

49. L'article 189 du Code de commerce dispose que « *les obligations nées à l'occasion de leur commerce entre commerçants ou entre commerçants et non-commerçants se prescrivent par dix ans si elles ne sont pas soumises à des prescriptions plus courtes* ». Il est donc possible pour un prestataire de service de paiement de conserver les données personnelles qui pourraient lui être nécessaires dans le cadre d'un litige avec le client. Seules les données personnelles en lien avec l'exécution des contrats et les services fournis par le responsable du traitement devront être conservées pour cette finalité.

Exemple 5 : Seules les données nécessaires à l'exécution du contrat entre une banque et son client (par exemple, un arrêté de compte) pourront être conservées après la clôture de du compte de la personne concernée afin de se constituer une preuve en cas de contentieux, dans la limite du délai de prescription de l'article 189 du Code de commerce (10 ans). En revanche, les données collectées dans le cadre des obligations de vigilance de la banque prévues par la Loi de 2004, telles que des données collectées à partir de « *watchlists* », devront être effacées au bout de 5 ans (en l'absence de période de conservation prolongée de 5 ans), conformément à l'article 3.6, alinéa 4 de la Loi de 2004 (« *Sans préjudice des délais de conservation plus longs prescrits par d'autres lois, les professionnels sont tenus d'effacer les données à caractère personnel à l'issue des périodes de conservation visées à l'alinéa 1er*».) et à l'article 3.6bis, alinéa 2 (« *Le traitement des données à caractère personnel sur la base de la présente loi pour toute autre finalité est interdit*. »).

[21] *EDPB Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, Version 1.0, Adopted on 8 October 2024* (cette version des lignes directrices est soumise à consultation publique).
[22] Avis de la Commission nationale pour la protection des données relatif au projet de loi n°7945 portant transposition de la directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union, Délibération n°49AV25/2022 du 21 octobre 2022 (p.22)

iii. Conservation des données d'un client pour la finalité de prévention de la fraude

50. La prévention de la fraude est indiquée dans le considérant 47 du RGPD comme l'un des intérêts légitimes possibles protégés par l'article 6.1 (f) du RGPD.

51. Concernant plus particulièrement les prestataires de services de paiement, il convient de rappeler les dispositions de l'article 105 de la Loi de 2009 : « *Les systèmes de paiement et les prestataires de services de paiement sont autorisés à traiter les données à caractère personnel lorsque cela est nécessaire pour garantir la prévention, la recherche et la détection des fraudes en matière de paiements*. […]»[23].

52. Dans le cadre de ses lignes directrices relatives à l'interaction entre la deuxième directive sur les services de paiement et le RGPD[24], le CEPD a rappelé que le traitement de données à caractère personnel strictement nécessaire à des fins de prévention de la fraude peut constituer un intérêt légitime du prestataire de services de paiement concerné, pour autant que les intérêts ou les libertés et droits fondamentaux de la personne concernée ne prévalent pas sur ces intérêts. Les activités de traitement à des fins de prévention de la fraude devraient alors reposer sur une évaluation approfondie au cas par cas par le responsable du traitement, conformément au principe de responsabilité.

53. Par ailleurs, le CEPD a, dans ses lignes directrices sur l'intérêt légitime, indiqué que le traitement des données personnelles dans le cadre de l'intérêt légitime de prévention de la fraude ne s'applique pas sans conditions ni limites, notamment parce que ce type de traitement peut avoir un impact significatif sur les personnes concernées. Par exemple, le considérant 47 du RGPD précise que le traitement des données personnelles doit être « *strictement nécessaire à des fins de prévention de la fraude* », ce qui doit être examiné conjointement avec le principe de minimisation des données inscrit à l'article 5.1 (c) du RGPD. Le CEPD indique également qu'en même temps, le principe de limitation de la conservation, prévu à l'article 5.1(e) du RGPD, doit être pris en compte lors de la définition des politiques de conservation des données applicables aux données traitées à des fins de détection ou de prévention de la fraude[25].

54. En pratique, le traitement mis en œuvre à des fins de contrôle et de lutte contre la fraude se traduit par un profilage au moyen d'algorithmes qui utilisent l'ensemble des données

[23] Il est probable que la base de licéité pour ce type de traitement soit à l'avenir l'obligation légale (article 6.1(c) du RGPD) : cf. article 83 de la Proposition de Règlement concernant les services de paiement dans le marché intérieur et modifiant le règlement (UE) nº 1093/2010. Il est intéressant de noter que l'article 83 de la Proposition dispose : « *Les prestataires de services de paiement ne stockent pas les données mentionnées au présent paragraphe plus longtemps que nécessaire aux fins énoncées au paragraphe 1, ni après la cessation de la relation avec le client*. ».

[24] Lignes directrices 6/2020 relatives à l'interaction entre la deuxième directive sur les services de paiement et le RGPD, version 2.0, adoptées le 15 décembre 2020

[25] *EDPB Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, Version 1.0, Adopted on 8 October 2024*, point 104 (cette version des lignes directrices est soumise à consultation publique).

disponibles pour calculer un taux de risque de fraude ou d'erreur pour chaque client (par exemple sur base d'un historique des fraudes déjà commises). Tout en reconnaissant pleinement l'importance de la lutte contre la fraude en matière de paiements, la CNPD souhaite néanmoins rappeler la très grande prudence avec laquelle ces algorithmes doivent être conçus et utilisés, eu égard aux risques qu'ils présentent et aux biais dont ils peuvent faire l'objet.

55. Dans un contexte en ligne, ce type de traitement peut impliquer la collecte de données relatives aux transactions mais aussi de données liées au contexte d'une opération de paiement telles que des données comportementales (analyse comportementale telle que la dynamique de frappe au clavier, des données liées aux habitudes d'achat et de consommation), des données de navigation et de connexion aux systèmes d'information (données de géolocalisation, données relatives au matériel : adresse IP, paramètre de l'écran ou du navigateur…).

56. La prévention, la recherche et la détection des fraudes en matière de paiements peut impliquer différents types de traitement tels que la détection d'actes présentant une anomalie ou une incohérence, la gestion et l'analyse de ces alertes, la constitution de listes de personnes dûment identifiées comme auteur d'actes qualifiés de fraude ou de tentative de fraude qualifiées comme telle par le responsable du traitement. Ces traitements peuvent être qualifiés de « profilage » au sens du RGPD[26]. Bien qu'il puisse y avoir des avantages à conserver les données dans le cas du profilage, puisqu'il y aura plus de données dont l'algorithme pourra s'inspirer, les responsables du traitement doivent respecter le principe de minimisation des données lorsqu'ils collectent des données à caractère personnel et veiller à ce qu'ils ne conservent ces données à caractère personnel que le temps nécessaire et proportionné aux finalités pour lesquelles ces données sont traitées[27].

57. Au vu de ce qui précède, la CNPD estime que la durée de conservation des données dans le cadre de la prévention et de la détection de la fraude devra être limitée au temps strictement nécessaire à l'accomplissement de cette finalité. Par exemple, la conservation des données d'une personne concernée pour laquelle aucune fraude n'a été détectée pendant la durée du contrat après la clôture de son compte ne semble ni nécessaire, ni proportionnée. Dans cette hypothèse, la CNPD estime que le responsable du traitement devrait effacer (ou anonymiser) les données traitées pour lutter contre la fraude après la fin de la relation contractuelle avec le client.

---

[26] Le profilage est défini comme « *toute forme de traitement automatisé de données à caractère personnel visant à évaluer les aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des aspects concernant le rendement au travail de la personne concernée, sa situation économique, sa santé, ses préférences ou centres d'intérêt personnels, sa fiabilité ou son comportement, ou sa localisation et ses déplacements, dès lors qu'il produit des effets juridiques concernant la personne en question ou qu'il l'affecte de façon similaire de manière significative* » (cons . 71 du RGPD).

[27] Cf. Groupe de travail « Article 29 » sur la protection des données, Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679 (WP251rev.01, p.13).

3. Bonnes pratiques dans la mise en application du principe de limitation de la conservation

58. Conformément aux articles 5 et 25 du RGPD, le responsable du traitement doit mettre en œuvre, des mesures techniques et organisationnelles appropriées, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du RGPD, y compris des 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.

a. Mise en place d'un mécanisme de tri des données

59. Ainsi, le responsable du traitement doit mettre en place des mesures permettant de faire un tri des données traitées une fois la phase d'utilisation courante des données de la personne concernée terminée (ce qui coïncide par exemple avec la clôture du compte de l'utilisateur) pour ne conserver que les données personnelles qui sont pertinentes au vu des (nouvelles) finalités dans la cadre de la phase d'archivage. En effet, la conservation systématique et sans distinction de toutes les données d'un compte après la fin de la relation contractuelle avec la personne concernée n'est pas conforme au principe de la limitation de la conservation[28]. Ce mécanisme de « purge » peut se traduire par l'effacement ou l'anonymisation des données à caractère personnel qui ne sont pas nécessaires pour poursuivre les finalités de conservation des données.

60. Le responsable du traitement devrait ainsi prévoir la conservation des données dans une base de données dédiée à l'archivage (a) ou au moins prévoir une séparation logique dans la base de données active (b)[29].
    (a) Une séparation physique pourrait être faite par l'extraction des données du système d'information pour les conserver séparément dans une base d'archivage dédiée à laquelle seules des personnes spécifiquement habilitées pourront accéder. Dans ce cas, la base d'archivage devra comporter différentes fonctionnalités, telles que l'export, l'accès et la visualisation des données stockées. Ces fonctionnalités permettront à l'organisme d'être en mesure de répondre à la personne concernée en cas d'exercice de ses droits (droit d'accès, etc.).

    (b) Avec une séparation logique, les données restent dans la « base active » mais sont clairement identifiées et isolées des autres données par une limitation des habilitations afin de les rendre inaccessibles aux personnes n'ayant plus besoin de les traiter[30].

[28] Article 5.1 (e) du RGPD. Cf. Commission Nationale de l'Informatique et des Libertés, Délibération de la formation restreinte n°SAN-2024-002 du 31 janvier 2024 concernant la société DE PARTICULIER A PARTICULIER – EDITIONS NERESSIS
[29] Cf. Commission Nationale de l'Informatique et des Libertés, Délibération de la formation restreinte n° SAN-2022-018 du 8 septembre 2022 concernant le GIE INFOGREFFE
[30] Cf. Guide pratique de la CNIL sur les durées de conservation.

b. Mise en place d'un mécanisme de fermeture des comptes « inactifs »

61. Certains acteurs proposent leurs services financiers uniquement via la création d'un compte en ligne. La CNPD constate qu'il est fréquent que ces utilisateurs n'utilisent parfois plus ces comptes, sans pour autant les clôturer, ce qui conduit parfois à l'existence de comptes inactifs pour une durée indéfinie, l'absence de clôture empêchant alors de faire courir certaines durées de conservation. Grâce à la loi du 30 mars 2022 relative aux comptes inactifs, aux coffres-forts inactifs et aux contrats d'assurance en déshérence, entrée en vigueur en date du 1 juin 2022, le Luxembourg a mis en place pour la première fois un cadre juridique en matière de gestion des comptes inactifs. Le nouveau cadre juridique est applicable à « *tout compte à vue, compte d'épargne, compte de dépôt à terme ou remboursable avec préavis, compte-titres, dépôt fiduciaire ainsi que tous autres comptes ouverts auprès d'un établissement.* ». En revanche, les comptes de monnaie électronique au sens de la loi modifiée du 10 novembre 2009 relative aux services de paiement sont exclus du champ d'application de ce cadre juridique.

62. Afin qu'un traitement soit assorti de garanties nécessaires pour répondre aux exigences du RGPD, dont le principe d'exactitude et de la limitation de la conservation, les responsables du traitement devraient prévoir des mesures pour vérifier de manière régulière que le titulaire du compte ait encore la volonté de maintenir le compte en ligne et que les données y conservées soient exactes. Dans le cas de comptes où le solde serait à zéro, la CNPD recommande également d'établir un délai à l'issue duquel le compte sera considéré comme inactif et devra être clôturé (après en avoir informé la personne concernée). A cet égard, la CNPD considère qu'un délai de 5 ans apparaît proportionné[31].

[31] Cette recommandation est sans préjudice des dispositions prévues par la loi du 30 mars 2022 relative aux comptes inactifs, aux coffres-forts inactifs et aux contrats d'assurance en déshérence.

4. L'obligation d'informer les personnes concernées sur les durées de conservation

63. En vertu de l'article 12 du RGPD, le responsable du traitement doit fournir aux personnes concernées les informations relatives aux traitements effectués "*d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples […]*" lorsqu'il communique avec les personnes concernées.

a. Droit à l'information préalable

Les articles 13.2 (a) (Informations à fournir lorsque des données à caractère personnel sont collectées auprès de la personne concernée) et 14.2 (a) du RGPD (Informations à fournir lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée) imposent au responsable du traitement d'informer les personnes sur la durée de conservation des données (ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée). Des informations précises sur les durées de conservation, en ce qu'elles contribuent à assurer pour les personnes concernées la maîtrise sur le traitement de leurs données, sont en effet importantes pour garantir un traitement équitable et transparent[32].

64. Au vu de ces dispositions, la CNPD rappelle que les prestataires de service de paiements doivent être transparents sur les durées de conservation de données personnelles des utilisateurs, notamment suite à la clôture de leur compte. Cela implique également une information sur les bases de licéité appliquées pour la conservation de leurs données (la détermination de ces bases de licéité permettant, notamment, de déterminer leurs droits prévus par le RGPD). Lorsqu'il s'agit de l'article 6.1 (f) du RGPD, la nature de l'intérêt légitime poursuivi par le responsable du traitement devrait figurer dans les informations portées à la connaissance des personnes. De plus, l'obligation de transparence est renforcée lorsqu'il est question de traitement de catégories particulières de données à caractère personnel visées aux articles 9 et 10 du RGPD[33].

b. Droit à l'information lors de l'exercice des droits en cours de traitement

65. Le responsable du traitement doit également fournir des informations claires aux personnes concernées lorsque ces derniers exercent leurs droits, tels que les droits d'accès et à l'effacement (article 12.1 du RGPD).

[32] Cf. Commission Nationale de l'Informatique et des Libertés, Délibération de la formation restreinte n°SAN-2024-002 du 31 janvier 2024 concernant la société DE PARTICULIER A PARTICULIER – EDITIONS NERESSIS

[33] Footnote LDT EDPB Transparence

66. Lorsqu'une personne concernée s'adresse à un prestataire de services de paiement dans le cadre de l'exercice de ses droits RGPD et si la personne a des questions en lien avec la conservation de ses données (par exemple une demande d'effacement), le responsable du traitement devra alors être en mesure de délivrer des informations précises : finalités de la conservation, bases de licéité, évènement déclenchant la durée de conservation, date(s) exacte(s) de l'effacement, données pouvant être effacées et données devant être conservées (informations figurant déjà dans le registre de traitement du prestataire de services de paiement).

Exemple 6 : Un utilisateur (personne concernée) fait une demande d'effacement de toutes ses données (sur base de l'article 17.1 (a) du RGPD) auprès d'un prestataire de services de paiement après avoir résilié son contrat avec lui. Le prestataire de services de paiement, agissant en tant que responsable du traitement, ne pourra pas effacer une grande partie des données de la personne concernée au vu des obligations légales qui lui sont applicables (article 17.3 (b) du RGPD). Dans sa réponse à la personne concernée, les informations fournies par le responsable du traitement devront alors, conformément à l'article 12.1 du RGPD, être plus spécifiques que dans sa notice d'information et devront notamment contenir des développements relatifs aux dispositions légales applicables et aux catégories de données qui ne pourront pas être effacées. Une simple référence aux « obligations légales applicables dans le secteur financier » ne pourra pas être considérée comme suffisante au vu de l'article 12.1 du RGPD.

Exemple 7 : Pendant la phase d'archivage, un utilisateur (personne concernée) s'oppose, sur base de l'article 21.1 du RGPD et pour des raisons tenant à sa situation particulière, au traitement de ses données sur base de l'intérêt légitime du PSP. Après avoir éventuellement limité le traitement conformément à l'article 18.1 (d) du RGPD, le responsable du traitement devra soit **(i)** procéder à l'effacement des données en vertu de l'article 17.1 (c) du RGPD, soit **(ii)** démontrer qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice (article 21.1 du RGPD). C'est dans cette 2nde hypothèse qu'il appartient au prestataire de services de paiement de fournir à la personne concernée des informations précises sur le traitement et notamment sur les motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée.