Certification RGPD des sous-traitants - Projet de référentiel d'évaluation de la CNIL

Contribution à la consultation publique

Alliance Digitale

Introduction

Alliance Digitale est la principale association professionnelle des acteurs du marketing digital et de la publicité en ligne en France. Elle est issue du rapprochement de l'IAB France, de la Mobile Marketing Association France et de la Data Marketing Association.

L'association regroupe la grande majorité des acteurs du marketing digital en France, soit près de 300 entreprises réparties sur l'ensemble de la chaîne de valeur (agences médias et conseils, éditeurs et régies, acteurs de la logistique et du print, data providers et fournisseurs de solutions Tech (adtech, martech) et marques).

L'Alliance Digitale rassemble parmi ses membres des entreprises intervenant en tant que responsables de traitement, sous-traitants, ou occupant alternativement ces deux rôles selon leurs activités. L'association a ainsi pour vocation de répondre à l'ensemble des points abordés dans le projet de référentiel d'évaluation de la CNIL soumis à consultation publique.

Nous souhaitons avant toute chose saluer la présente initiative de la CNIL. L'instauration d'un mécanisme de certification, tel que prévu par l'article 42 du RGPD, constitue une avancée importante pour assurer une application cohérente du texte. L'Alliance Digitale a toujours eu à cœur de favoriser l'adoption de Codes de conduite et de dispositifs de certification, conformément aux dispositions de la Section 5 du RGPD.

Nous déplorons toutefois que, dans sa forme actuelle, la certification revête un caractère largement dissuasif pour les entreprises susceptibles d'y prétendre. Les coûts associés à la candidature (notamment liés à la mobilisation de ressources spécialisées pour réaliser des chantiers de conformité poussés allant au-delà de la réglementation applicable), ainsi que l'incertitude en ce qui concerne les conditions de sa suspension ou son retrait, risquent de dépasser largement les bénéfices attendus, limitant ainsi son attractivité et son adoption.

Ce constat est d'autant plus préoccupant pour les petites et moyennes entreprises, qui se trouveraient de facto exclues de cette certification si le niveau d'exigence requis demeure aussi élevé. Nous estimons que cela risque d'accentuer la fragmentation du marché, non pas sur la base du niveau de sécurité des traitements, mais en raison de considérations purement économiques et financières. Compte tenu de l'impact financier des sanctions prises sur le fondement du RGPD et de la pression règlementaire qui s'accentue autour de la relation entre le responsable de traitement et le sous-traitant, l'absence de certification risque être perçue

comme une non-conformité d'un sous-traitant. Une telle situation serait évidemment préjudiciable et ne ferait que renforcer les déséquilibres existants sur le marché.

Nous appelons la CNIL à davantage prendre en considération cet élément et ce, conformément à l'article 42.1 du RGPD qui précise que « les besoins spécifiques des micro, petites et moyennes entreprises sont pris en considération ».

Enfin, le projet de référentiel d'évaluation gagnerait ainsi à trouver un équilibre plus satisfaisant entre, d'une part, le niveau de précision requis pour garantir la rigueur et l'homogénéité de l'évaluation menée par l'organisme de certification et assurer la conformité du sous-traitant aux exigences de la certification, et, d'autre part, la flexibilité nécessaire pour permettre aux entreprises de s'adapter aux réalités opérationnelles et aux spécificités de leur activité.

Vous trouverez ci-dessous la réponse de Alliance Digitale à la consultation publique. Celle-ci s'organise sur la base de remarques générales qui constituent des enjeux majeurs pour nos membres et de remarques spécifiques plus détaillées qui suivent l'organisation du projet de référentiel d'évaluation de la CNIL.

Synthèse de la contribution et principales recommandations

Dans le cadre de la consultation publique sur le projet de référentiel d'évaluation, l'Alliance Digitale souhaite alerter principalement la CNIL sur :

- Le coût prohibitif de la certification : les frais associés à une candidature à la certification sont particulièrement élevés, notamment pour les petites et moyennes entreprises ne disposant pas de ressources internes dédiées, ce qui pourrait dissuader nombre d'entre elles de s'engager dans cette démarche ou le cas échéant, avoir un impact important sur leur capacité à investir à des fins d'innovation ;

- Le risque de fragmentation du marché : une telle situation pourrait accentuer la disparité entre grandes et petites et moyennes entreprises, voire entraîner l'exclusion de certaines petites structures si les obligations demeurent aussi contraignantes ;

- L'existence de critères excessivement dissuasifs : des exigences telles que la suspension des traitements en cas de retrait de la certification ou la périodicité imposée des audits techniques apparaissent particulièrement décourageantes. En outre, la suspension des traitements en cas de retrait de la certification semble indiquer que l'absence de certification pourrait correspondre *de facto* à une non-conformité du traitement / de « l'offre de service » avec le RGPD ;

- Une surinterprétation du RGPD : de nombreux critères semblent découler d'une interprétation excessive du RGPD, imposant des contraintes supplémentaires non prévues par le texte ;

- Une protection insuffisante du secret des affaires : le projet de référentiel d'évaluation ne prévoit pas de mesures suffisamment protectrices par rapport à l'ensemble des informations qui doivent être mises à disposition par les sous-traitants pour obtenir la certification ;

- Un manque de précision de certains critères : l'absence de clarté dans les attentes pour satisfaire les critères peut conduire à des interprétations divergentes, compromettant ainsi l'uniformité du processus.

Dans ce cadre et à l'aune des éléments ci-dessus, nous recommandons principalement à la CNIL de :

- Apporter des clarifications s'agissant du périmètre territorial et du cadre des activités/traitements susceptibles d'être certifiés ;

- Faciliter la lecture en évitant les nombreux renvois et en adoptant une approche thématique plutôt que chronologique, à l'instar de la certification des compétences du délégué à la protection des données ;

- Prendre en compte le coût financier, administratif et organisationnel pour les entreprises concernées afin de favoriser l'adoption de la certification ;

- De la même manière, mieux considérer les contraintes et moyens (y compris humains) des plus petites entreprises comme en dispose l'article 42.1 du RGPD ;

- Éviter une surinterprétation systématique du RGPD et renoncer aux critères les plus dissuasifs du projet de référentiel ;

- Tenir compte des travaux CEPD sur la notion de responsable de traitement et de sous-traitant de juillet 2021 et renoncer aux obligations qui viennent transférer des obligations juridiquement dévolues au responsable de traitement au sous-traitant ;

- Préciser et homogénéiser les définitions et terminologies utilisées tout au long du projet de référentiel pour assurer une compréhension uniforme et sans équivoque.

I. Remarques générales

- **Sur le périmètre**

Nous souhaiterions revenir sur deux dimensions principales du projet de référentiel d'évaluation de la CNIL :

- Le périmètre territorial et les questions qu'il pose ;

- Le cadre des activités/traitements susceptibles d'être certifiés.

S'agissant du périmètre territorial :

Nous comprenons tout d'abord qu'il concerne les organismes établis sur le territoire de l'Union européenne (UE) ou dans un État membre de l'Espace économique européen (EEE). Cela soulève plusieurs interrogations :

- Pourquoi exclure du périmètre un pays comme la Suisse qui fait partie de l'Association européenne de libre-échange (AELE) et dispose d'une décision d'adéquation de la Commission européenne tout comme le Royaume-Uni[1] ? Si l'objectif de la certification est qu'elle soit un atout commercial pour les entreprises qui font le choix de s'investir pour la respecter, il est dommageable qu'elles ne puissent pas la faire valoir auprès de clients qui ne dépendent ni de l'UE ni de l'EEE ;

- Par ailleurs, pourquoi limiter aux organismes établis sur le territoire de l'UE ou de l'EEE ? Un sous-traitant opérant en dehors de l'UE ou de l'EEE adressant des services au sein de l'un des deux espaces (ou les deux) doit également appliquer le RGPD de la même manière. Nous ne voyons pas dès lors pourquoi ils seraient privés de certification. Par ailleurs, cela pourrait priver certaines entreprises françaises disposant de filiales ou d'une maison mère en dehors de l'EEE (ex. une société française ayant une filiale établie au Royaume Uni ou au Canada) et qui agiraient comme sous-traitant de l'établissement principal ou d'autres responsables de traitement d'accéder à ladite certification.

Nous comprenons en outre que la certification vise à offrir aux responsables de traitement un moyen de sélectionner des sous-traitants présentant des garanties suffisantes en matière de protection des données à l'échelle de l'Union européenne. Elle serait ainsi applicable à l'ensemble des marchés européens et ce, indépendamment de l'octroi par le Comité européen

[1] Adéquation de la Suisse par l'UE, 15 janvier 2024, https://www.bj.admin.ch/bj/fr/home/staat/datenschutz/internationales/angemessenheit-ch.html#:~:text=Le%2015%20janvier%202024%2C%20la,adéquat%20de%20protection%20des%20données ;
Adéquation du Royaume-Uni, 01 juillet 2021, https://www.cnil.fr/fr/brexit-la-commission-europeenne-adopte-des-decisions-relatives-ladequation-du-niveau-de-protection

de la protection des données (CEPD) du « label européen de protection des données[2] », qui n'est étrangement pas mentionné dans le projet de référentiel d'évaluation de la CNIL ou dans la communication qui l'accompagne. Cela soulève plusieurs questions :

- La CNIL entend-elle soumettre les critères de son référentiel au CEPD afin d'en faire une certification commune conformément à l'article 42.5 du RGPD ? Si oui, dans quelle temporalité et quelles étapes seraient nécessaires ? Si cette certification n'a pas vocation à être commune, ne serait-il pas opportun néanmoins qu'elle soit soumise pour avis au CEPD ? ;

- Quelle serait la valeur de la certification auprès des autres autorités de protection des données ? Certaines d'entre-elles sont-elles impliquées dans les travaux en cours de la CNIL ? Si cette dernière souhaite promouvoir son propre référentiel à travers l'UE, envisage-t-elle de le traduire dans l'ensemble des langues pertinentes afin que toutes les entreprises européennes puissent en bénéficier ?

- La CNIL a-t-elle envisagé le risque d'émergence d'un « conflit de certification » si une autre autorité de protection des données venait à effectuer le même exercice ? Et le cas échéant, quelle serait les mesures prises pour éviter une incertitude juridique importante pour les entreprises et toute forme de « certification shopping » ?

<u>S'agissant des activités/traitements susceptibles d'être certifiés</u>

Le projet de référentiel d'évaluation ne nous semble pas suffisamment clair quant à ce qu'il est possible de faire certifier. Ledit projet établit la distinction entre les traitements et les « offres de services » effectués en tant que sous-traitant. Il évoque également les notions de « prestation », « d'activité » de « service » ou encore de « configurations ».

Il est difficile de savoir assurément ce sur quoi les entreprises pourraient candidater à la certification *a fortiori* dans la mesure où le projet et les communications associées ne sont pas assortis d'exemples illustratifs.

En premier lieu, nous n'arrivons pas à comprendre si une entreprise serait en mesure de faire certifier plusieurs traitements d'un seul coup lorsque ceux-ci ne font pas partie d'une « offre de service » ou si chacun des traitements devrait faire l'objet d'un processus certification différent. De la même manière, si un sous-traitant obtient une certification pour un traitement ou une offre de service, doit-il reprendre l'intégralité du processus pour certifier un autre traitement ou une autre offre ou certains critères peuvent-ils être considérés comme déjà satisfaits ? Il s'agit d'un point important pour l'ensemble des membres de l'Alliance Digitale puisqu'un traitement ne

[2] Article 42.5 RGPD « *Une certification en vertu du présent article est délivrée par les organismes de certification visés à l'article 43 ou par l'autorité de contrôle compétente sur la base des critères approuvés par cette autorité de contrôle compétente en application de l'article 58, paragraphe 3, ou par le comité en application de l'article 63.* ***Lorsque les critères sont approuvés par le comité, cela peut donner lieu à une certification commune, le label européen de protection des données***. »

correspond pas nécessairement à une prestation fournie par un sous-traitant à son responsable de traitement.

Une autre question concerne l'impact potentiel de l'évolution d'un traitement certifié sur la validité de sa certification. Il est essentiel de clarifier dans quelle mesure une modification des modalités d'un traitement pourrait entraîner la perte de cette certification, qu'il s'agisse d'un traitement certifié de manière autonome ou intégré dans une offre de service.

En second lieu, la définition « d'offres de service » et ses implications dans le processus de certification ne nous semblent également pas suffisamment claires alors même que des obligations additionnelles sont prévues par le référentiel d'évaluation dans ce cadre. La qualification « sur étagère » ne renvoie tout d'abord pas à des éléments tangibles pour les membres de l'Alliance Digitale. Cela renvoie à plusieurs questions : s'agit-il d'un produit similaire fourni par un sous-traitant à plusieurs responsables de traitement ? Est-ce que ledit produit peut être modifié dans ses fonctionnalités et paramètres sans impact sur l'obtention de la certification ? Une entreprise pourrait-elle faire certifier de façon globale une offre dite de « service » qui comprendrait plusieurs configurations, types de prestation et traitements différents ? Il s'agit également d'un point important pour les entreprises fournissant plusieurs « offres de service » et la réponse apportée par la CNIL pourrait conditionner l'attractivité de la certification pour ces dernières.

La réponse claire à l'ensemble de ces questions est indispensable pour permettre aux entreprises de bien appréhender ce qu'ils seraient en mesure de faire certifier, comment et surtout, à quel coût pour l'entreprise.

- **Sur la faisabilité d'obtenir la certification**

D'un point de vue général, ce point constitue l'un des aspects les plus problématiques du projet de référentiel d'évaluation dans sa version actuelle.

Nous souhaitons alerter la CNIL sur le fait qu'à ce jour, seule une infime minorité d'entreprises serait potentiellement en mesure de se conformer aux 90 obligations définies dans le projet de certification. Les TPE/PME en seraient assurément exclues. Nous le regrettons d'autant plus que ce dispositif revêt une importance majeure pour une application effective du RGPD et qu'il s'agit de la première initiative de cette nature portée par la CNIL.

La multiplication d'obligations allant au-delà des exigences des textes légaux et règlementaires applicables, comme nous le détaillons dans la seconde partie de cette note, rend cette démarche largement dissuasive. L'ampleur des coûts associés, la charge documentaire excessive, la non-définition des conséquences des modifications ou évolutions des prestations certifiées sur la validité de la certification et le peu de marge de manœuvre laissée au sous-traitant, risquent de transformer cette certification en un dispositif réservé à quelques acteurs, et donc contraire à l'objectif d'une adoption large et effective.

Par ailleurs, la complexité de lecture du référentiel est accentuée par de fréquents renvois à d'autres critères, créant une interdépendance entre ces derniers et compliquant sa compréhension. Il est souvent difficile de déterminer si l'accomplissement d'un critère

conditionne l'obtention d'un autre. Une approche thématique (par exemple : enjeux contractuels, gouvernance, transparence, mesures de sécurité), à l'instar de celle adoptée dans le référentiel de certification des délégués à la protection des données[3], nous semblerait plus pertinente que l'approche strictement chronologique retenue en l'espèce.

Enfin, afin de faciliter la compréhension et l'adoption de cette certification, le projet devrait donner une indication sur les livrables à fournir pour satisfaire aux critères ainsi que clarifier de façon explicite le niveau de granularité attendu. À ce stade, ces éléments demeurent insuffisamment précisés.

- **Sur l'intérêt des sous-traitants à l'obtention de la certification**

Plusieurs éléments nous amènent à penser que le dispositif, dans sa forme actuelle, ne constitue pas une incitation suffisante pour les entreprises. Son adoption risque ainsi de rester limitée, en raison d'un manque de clarté sur le périmètre de la certification, d'un déséquilibre entre les exigences imposées et les bénéfices attendus, ainsi que de l'absence de définition précise des conditions de maintien de la certification en cas de modification.

Il nous parait dommage que la certification ne garantisse ni la validité d'un traitement ni une conformité au RGPD. Elle ne semble pas non plus pouvoir être invoquée comme un facteur atténuant en cas de contrôle ou de contentieux, ce qui en limite fortement l'intérêt pour les entreprises.

Par ailleurs, la certification, dans sa forme actuelle, ajoute une couche supplémentaire de complexité conformité, augmentant ainsi la charge réglementaire pesant sur les entreprises. La mise en conformité avec un tel référentiel engendre un surcoût perpétuel difficilement soutenable, en particulier pour les acteurs économiques de moindre taille. Cette contrainte financière et organisationnelle réduit considérablement l'attractivité du dispositif et risque, en pratique, d'en limiter l'adoption.

Un autre frein majeur réside dans l'impact des évolutions des produits et services sur la validité de la certification. Si le projet de référentiel d'évaluation s'aligne sur l'article 42.7 du RGPD en prévoyant le retrait de la certification lorsque les exigences ne sont plus satisfaites, il va toutefois au-delà en imposant la suspension des traitements concernés, comme si le non-respect d'un critère du référentiel était présumé constituer une infraction grave au RGPD. Une telle exigence introduit une incertitude juridique significative avec des impacts économiques et opérationnels pour les entreprises, largement susceptibles de les dissuader de s'engager dans ce processus puisque les exposant à davantage de risques que la réglementation applicable.

Enfin, l'incertitude sur les conséquences d'une modification de produit/d'un service sur la certification constitue un frein majeur. Si une simple évolution peut entraîner la perte de la certification, cela devient un facteur de rigidité incompatible avec la réalité des entreprises, qui ont besoin de flexibilité pour faire évoluer leurs produits et services.

[3] Délibération n° 2018-318 du 20 septembre 2018 portant adoption des critères du référentiel de certification des compétences du délégué à la protection des données (DPO) https://www.cnil.fr/sites/cnil/files/2023-08/deliberation_n2018-318_du_20_septembre_2018_consolidee.pdf

- **Sur le risque de fragmentation du marché européen**

La certification, telle qu'elle est envisagée dans ce projet de référentiel, risque d'être difficilement accessible pour la plupart des entreprises, car elle impose des exigences allant au-delà du cadre du RGPD et des autres textes légaux applicables. Cette situation pose deux problèmes majeurs.

D'une part, l'élévation du niveau des exigences risque de limiter drastiquement le nombre d'entreprises pouvant obtenir cette certification. En l'état, certaines catégories d'acteurs, notamment les TPE et PME, pourraient se retrouver de facto exclues du processus, faute de ressources suffisantes pour répondre aux critères imposés (par exemple : l'embauche d'un juriste RGPD / DPO à temps plein sur les sujets de conformité, ou le recours à des cabinets de conseil). Or, cette approche semble contraire à l'article 42.1 du RGPD, qui précise que « les besoins spécifiques des micro, petites et moyennes entreprises sont pris en considération ».

D'autre part, le risque d'une distorsion concurrentielle est réel. Si la certification venait à être perçue comme une norme de marché, il est à craindre que certains responsables de traitement en fassent une condition incontournable pour contractualiser avec leurs sous-traitants. Une telle évolution reviendrait à exclure du marché des entreprises dont les traitements seraient pourtant conformes au RGPD, mais qui n'auraient pas les moyens financiers ou organisationnels d'obtenir la certification.

Par ailleurs, ce risque est renforcé par la conséquence de la perte de certification, à savoir l'obligation de cesser le traitement, qui semble indiquer que l'absence de certification équivaudrait automatiquement à une non-conformité au RGPD.

Afin d'éviter ces écueils, nous recommandons à la CNIL d'adopter une approche plus pragmatique, reposant sur deux leviers complémentaires :

- Premièrement, il est essentiel de rendre cette certification plus accessible en limitant ses exigences aux seules obligations prévues par le RGPD, sans ajouter de contraintes supplémentaires qui ne seraient pas imposées par une obligation légale ou réglementaire. Si des exigences supplémentaires existent, il serait judicieux de les identifier clairement comme telles, en les distinguant des critères de conformité au RGPD. Celles-ci pourraient par exemple être qualifiées de souhaitables mais non obligatoires pour obtenir la certification. Plus de détails sont accessibles dans la seconde partie du document sur ce point ;

- Deuxièmement, la CNIL devrait intégrer une approche modulable selon la taille des entreprises, à l'instar d'autres mécanismes de certification, et/ou des risques présentés par les traitements afin d'assurer une plus grande équité et de ne pas pénaliser les plus petites structures.

- **Sur les risques d'interprétation différente des organismes de certification**

De nombreux critères du projet de référentiel manquent de précision ou ne sont pas suffisamment clairs (voir détails dans la seconde partie), notamment s'agissant de l'exigence de

granularité. Cette absence de clarté ouvre la porte à des interprétations divergentes, ce qui présente un risque : selon la manière dont chaque organisme de certification interprète les critères de la certification, l'approche appliquée pourrait varier d'un organisme à l'autre.

Une telle situation entraînerait une application non homogène de la certification, remettant ainsi en cause son objectif même de standardisation et de fiabilité. Pour éviter ces incohérences, il est essentiel que la version finale du référentiel rédigée par la CNIL apporte des clarifications précises, garantissant ainsi une application uniforme des exigences. Il serait aussi judicieux de d'inclure des exemples concrets des informations que les organismes de certification ne doivent pas exiger, afin de clarifier les limites de leurs demandes.

- **Sur le transfert d'obligations du responsable de traitement au sous-traitant**

Le projet de référentiel d'évaluation impose aux sous-traitants des responsabilités allant au-delà de ce que prévoit le RGPD. De nombreux critères transfèrent en outre au sous-traitant des obligations qui relèvent traditionnellement du responsable de traitement, ce qui constitue un changement majeur.

Au-delà des préoccupations déjà exprimées sur le risque de faible adoption du dispositif, cette complexification des obligations des sous-traitants pourrait brouiller davantage la frontière entre leur rôle et celui de responsable de traitement conjoint. Cela interroge sur une éventuelle volonté de la CNIL d'encourager ce régime, alors même que cette tendance se manifeste déjà dans certaines pratiques contractuelles observées parmi les membres d'Alliance Digitale. La certification, telle que proposée, risque d'amplifier ce glissement et de fragiliser les entreprises concernées.

- **Sur la protection du secret des affaires**

Le projet de référentiel gagnerait à être davantage protecteur des informations des sous-traitants, notamment en ce qui concerne l'ensemble des informations devant être mises à disposition pendant la phase précontractuelle (dont la définition, notamment dans le cadre du critère C1.05, reste floue à nos yeux). En effet, ces informations sont souvent confidentielles et d'une grande importance pour les activités des sous-traitants, ce qui soulève des préoccupations en matière de confidentialité, de sécurité et de sauvegarde du modèle économique de certains prestataires. Dans la phase précontractuelle, si l'on considère qu'un prestataire démarche un client potentiel sans qu'aucun engagement commercial n'ait été pris, le prestataire agissant en tant qu'intermédiaire s'expose à un risque significatif en révélant l'identité de ses sous-traitants à l'entreprise prospectée. En effet, cette dernière pourrait contourner le prestataire intermédiaire en contractant directement avec les sous-traitants identifiés, profitant ainsi de la phase précontractuelle pour obtenir ces informations sans finaliser de contrat avec le prestataire initial. A noter que ce risque est largement compensé lorsque le prospect devient client, via la conclusion au contrat de prestations de clauses de non-sollicitation de sous-traitants (voir critère C1.05).

La version finale devrait renforcer la protection des informations mises à disposition par le sous-traitant aux prospects, clients ainsi qu'à l'organisme de certification. Enfin, nous considérons

également nécessaire qu'une clause spécifique sur le sujet soit spécialement dédiée aux informations transmises à l'organisme de certification, ce qui n'est pas le cas en l'état actuel de la rédaction.

- **Sur les définitions et terminologies utilisés**

Plusieurs définitions, terminologies et termes utilisés pourraient être précisés afin de renforcer la bonne compréhension du projet de référentiel d'évaluation de la CNIL. En voici les principaux :

- Entité juridique : la définition qui est donnée interdit aux personnes physiques de candidater à la certification ;
- Établissement : le projet de référentiel d'évaluation utilise le terme « établissement » sans préciser la définition juridique sur laquelle il s'appuie (voir critère C0.02) ;
- Flux de données : notion nouvelle non définie dans le RGPD et importante s'agissant du critère C0.08 et la « cartographie des flux » dont le sous-traitant doit disposer ;
- Vulnérabilité critique : il est nécessaire de développer ce point qui n'est défini nulle part dans la réglementation applicable et n'est pas clair en l'espèce ;
- Phase précontractuelle : il faudrait définir ce terme qui ne l'est pas dans la rédaction actuelle. Il peut renvoyer à deux réalités différentes selon l'état d'avancement avec un prospect (voir C1.05) ;
- Offre de service : la présente définition et notamment le terme « sur étagère » mérite d'être clarifié d'autant plus que les « offres de service » font l'objet d'obligations supplémentaires. Il serait utile également de préciser si cela correspond à une « offre standardisée » telle qu'établie par les lignes directrices du CEPD concernant les notions de responsable de traitement et de sous-traitant dans le RGPD[4] et de définir les limites des options de personnalisation d'une offre standardisée afin qu'elle conserve son caractère "sur étagère» ;
- Intérêt administratif : notion nouvelle non définie et utilisée dans au moins deux critères (C0.05, C1.16). Il est important de clarifier ce qui est entendu ici et de l'illustrer avec des exemples concrets.

Il serait également opportun d'homogénéiser le vocabulaire utiliser et/ou de préciser une fois exactement ce qui est entendu. Nous pensons spécifiquement à l'utilisation fréquente de :

- « En particulier » pouvant donner lieu à plusieurs interprétations et ouvrant la voie à des situations différentes selon celle choisie par l'organisme de certification. Il serait opportun de clarifier la différence de ce terme avec le « notamment » et le « a minima » présents également fréquemment dans des dispositions similaires. Il pourrait être judicieux d'inclure des exemples concrets de ce qui ne doit pas être exigé en tant que critère de certification, afin de clarifier les attentes et d'éviter les exigences excessives ou non pertinentes ;

[4] Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, Juillet 2021 https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_fr.pdf

- « Doit disposer », « mis à disposition » : besoin de clarifier ce qui doit être disponible sur demande (par exemple lors d'un audit) de ce qui doit être fourni publiquement.

II. Remarques spécifiques

Cette section expose en détail les points soulevant les principales préoccupations des membres d'Alliance Digitale ou nécessitant des clarifications. Chaque observation est accompagnée d'une recommandation formulée en conséquence.

Afin d'assurer une meilleure lisibilité, les éléments sont présentés sous forme de tableaux, en suivant l'organisation retenue par la CNIL dans son projet de référentiel d'évaluation.

Partie 0 : La demande de certification du sous-traitant – l'éligibilité

Plan du projet de référentiel	Commentaires Alliance Digitale
C0.01	Le périmètre dont il est question ici exclut *de facto* les entreprises qui disposent de filiales, de sièges ou d'une maison mère en dehors de l'Union européenne et celles qui ont adopté des « règles d'entreprises contraignantes[5] » pour garantir un niveau de protection adéquat[6]. Le RGPD impose des obligations aux sous-traitants établis en dehors de l'UE dès lors qu'ils traitent des données personnelles pour le compte d'un responsable de traitement soumis au règlement. Dès lors, priver ces sous-traitants non européens du droit à la certification pourrait créer une forme de discrimination, en les soumettant aux mêmes obligations sans leur offrir les mêmes opportunités de reconnaissance de conformité. Nous souhaiterions que la CNIL modifie ce point.
C0.02	Même remarque ici. Sur la notion « d'établissement », nous avons besoin de précisions : le terme « établissement » inclut-il une filiale ou une entité affiliée, ou se limite-t-il à un simple bureau ? Ce critère pourrait potentiellement exclure du programme de certification des sociétés européennes ayant des filiales, des sièges ou une maison mère hors de l'UE. Exemple : la société A, établie dans l'UE, possède une filiale au Royaume-Uni qui exerce la même activité économique. Le personnel de cette filiale a accès

[5] Binding Corporate Rules (BCR)

[6] Il y a donc deux types de sociétés exclues : les sous-traitants français ou européennes avec des établissements non européens et les sous-traitants non-européens.

	aux données traitées par la société A. Par ailleurs, la filiale au Royaume-UNi agit comme sous-traitant pour la société B. Dans ce cas, la société A est-elle exclue du programme de certification ? Si oui, pour quelle raison ? Nous souhaiterions que la CNIL clarifie la manière dont cette responsabilité s'applique aux organisations ayant des structures décentralisées ou des unités commerciales indépendantes.
C0.03	Les obligations identifiées ici pour le sous-traitant nous semblent poser plusieurs problématiques : - <u>Certaines obligations ne sont pas applicables à tous les services opérés</u> : Il n'y a par exemple pas toujours des transferts hors UE mis en œuvre ni même nécessairement de processus d'anonymisation mis en place et encore moins de sous-traitants ayant systématiquement accès aux systèmes d'information ; - <u>Des éléments obligatoires et facultatifs sont placés au même niveau</u> : c'est le cas par exemple du processus d'anonymisation ou de l'identification de l'ensemble de ses potentiels sous-traitants ultérieurs. Par ailleurs, des informations telles que les établissements où le traitement est effectué et les détails concernant l'accès privilégié aux locaux ou aux systèmes peuvent ne pas démontrer directement le respect des obligations du RGPD. Cela pourrait imposer une charge administrative excessive aux sous-traitants ; - <u>La liste des dispositions législatives et réglementaires à respecter emporte un risque important de sécurité juridique :</u> il est compliqué de lister de façon exhaustive l'ensemble des dispositions applicables en matière de protection des données. Par ailleurs, le critère ne précise pas les conséquences d'un oubli sur le respect du critère et *a fortiori* de la certification ni même de la conséquence d'une évolution de la loi. Devrait-il y avoir une mise à jour obligatoire ? Et le cas échéant, en attendant cette mise à jour, les traitements devraient-ils être suspendus ? ; - <u>Un risque existe pour la confidentialité :</u> en plus de reposer sur aucune base légale ou réglementaire, le c) emporte des risques de confidentialité tant il exige la mise à disposition, dans le cadre de la certification, d'informations sensibles pour le sous-traitant. Nous recommandons ainsi de :

	- Préciser que certains critères ne doivent être remplis que si cela est pertinent pour l'activité du sous-traitant en question en ajoutant par exemple la formulation « le cas échéant » ; - Se contenter des obligations issues du RGPD ; - Préserver la confidentialité des informations des entreprises afin de promouvoir l'adoption de la certification ; - Renoncer à la liste des dispositions législatives et réglementaires auxquelles le sous-traitant serait soumis lorsqu'il effectue des traitements pour le compte de son client qui est trop complexe et emporte une incertitude juridique élevée pour les entreprises.
C0.03 bis	Même remarque concernant le b) que pour le f) du C0.03. L'exigence faite au sous-traitant de dresser la liste de tous les services proposés aux clients pourrait aller au-delà des exigences de l'article 28 du RGPD et poser des difficultés aux sous-traitants qui proposent un large éventail de services, en particulier dans les secteurs dynamiques où les offres de services sont fréquemment mises à jour. Par ailleurs, en obligeant les sous-traitants à identifier et à répertorier les réglementations nationales ou européennes applicables à leurs clients, l'article risque de transférer une partie de la responsabilité du responsable du traitement au sous-traitant. En vertu du RGPD, les responsables du traitement sont les premiers responsables de la détermination de la base juridique et du cadre de conformité applicable à leurs opérations de traitement (articles 5 et 6 du RGPD). Cette exigence pourrait brouiller la répartition des responsabilités entre les responsables du traitement et les sous-traitants. De plus, le terme « loi nationale » devrait être plus clairement défini : que se passe-t-il lorsque le service est présent dans plusieurs Etats-membres ?
C0.04	L'impossibilité pour les sous-traitants de faire certifier leurs traitements ou offres de services destinés à des responsables de traitement non soumis au RGPD apparaît comme une limite dommageable. Elle prive ces acteurs des bénéfices potentiels de la certification et restreint, par conséquent, la diffusion des principes de protection de la vie privée qu'un tel dispositif pourrait pourtant encourager à une échelle plus large. Par ailleurs, le projet n'aborde pas la question des situations dans lesquelles un sous-traitant opère à la fois dans le cadre du RGPD et de la directive 2016/680 relative à l'application de la loi pour différentes activités de traitement. Par exemple, un sous-traitant fournissant des services à la fois à des entreprises privées (RGPD) et à des organismes chargés de la prévention et de la détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, peut être confronté à une ambiguïté concernant l'applicabilité de la certification.

	Nous souhaiterions que la CNIL prenne en considération ces éléments.
C0.05	Ce critère emporte plusieurs éléments problématiques. Le premier point d'attention porte sur l'objectif même du critère, qui ne s'applique pas spécifiquement au sous-traitant en tant que tel, mais aux traitements qu'il met en œuvre en qualité de responsable de traitement. Outre la charge et le coût induit par l'application de ces obligations, l'exigence de recenser l'ensemble des traitements non liés à son activité de sous-traitance semble inappropriée dans un référentiel censé lui être dédié. Par ailleurs, les informations requises nous paraissent non pertinentes, notamment s'agissant de la description des traitements effectués en tant que responsable de traitement dans le cadre d'une certification qui peut restreindre la capacité d'adapter ces traitements, limitant ainsi sa liberté dans la définition de ses processus. C'est d'ailleurs le principe même des qualifications responsable de traitement/sous-traitant/responsable conjoint tel que définies par le RGPD et précisées par les lignes directrices du CEPD[7]. En outre : - Nous ne comprenons pas le sens et la portée du a) qui nous apparait déconnecté des réalités de l'activité des sous-traitants, à tout le moins dans le secteur du marketing digital et de la publicité en ligne. Par ailleurs, les éléments suivants : « les traitements (…) ne vise pas spécifiquement le traitement de données à caractère personnel » nous apparaissent incohérents avec le critère C0.04 qui dispose que seuls les traitements soumis au RGPD sont concernés ; - L'introduction d'une notion dite d'« intérêt administratif » dans le c) nous apparait peu précise quant à ce qu'elle pourrait recouvrir et déconnectée là-aussi du processus de certification. Nous recommandons à la CNIL ici de renoncer à ce critère qui est décorrélé de l'objectif et du périmètre de son projet de référentiel d'évaluation.
C0.06	Plusieurs éléments à relever également ici : - Ce critère ne semble relever d'aucune obligation légale ;

[7] Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, Juillet 2020, Voir exemple p. 27 « Chasseurs de tête » (Toutefois, l'entreprise X est le seul responsable du traitement nécessaire à la gestion de sa base de données et l'entreprise Y est le seul responsable du traitement ultérieur de recrutement pour sa propre finalité (organisation d'entretiens, conclusion du contrat et gestion des données RH »). https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_fr.pdf

	- Le sous-traitant ne dispose pas des informations requises pour respect ce critère : ce n'est pas le sous-traitant qui choisit d'effectuer une prise de décision automatisée comme indiquée dans le b). Il ne sait pas forcément non plus dans quel objectif les données personnelles sont utilisées comme le a) le laisse prétendre (l'article 4 du RGPD disposant expressément que c'est le responsable de traitement qui détermine les finalités d'un traitement – c'est d'ailleurs un critère clé qui distingue une entité responsable de traitement d'une sous-traitante) ; - Un renforcement inquiétant du rôle du sous-traitant : ce critère est inquiétant car il tend à brouiller la frontière entre le responsable de traitement et le sous-traitant. Cela nous parait juridiquement dangereux car le sous-traitant n'a aucune garantie contractuelle de l'utilisation des données personnelles qui est faite par son ou ses client(s) responsable(s) de traitement. De plus, exiger des sous-traitants qu'ils communiquent ces informations implique que l'on s'attend à ce qu'ils aient une responsabilité supplémentaire en matière d'identification et d'évaluation des risques, ce que le RGPD attribue en premier lieu aux responsables du traitement ; - Absence de sécurité juridique : le critère ne précise pas les conséquences pour un sous-traitant dans l'hypothèse où le responsable de traitement manquerait à ses obligations ou ne justifierait pas de façon acceptable (quels critères ?) le fait qu'il ne dispose pas des informations demandées. Une incertitude demeure quant à l'impact d'un tel manquement sur la certification du sous-traitant, alors même que celui-ci n'en est pas responsable. Cette absence de clarification soulève un risque important pour les sous-traitants, qui pourraient voir leur certification remise en cause sans qu'ils aient eux-mêmes failli à leurs obligations ; - Les critères ne sont pas suffisamment précis : notamment le h) s'agissant de « l'usage innovant » qui n'est pas bien défini. Par ailleurs, nous contestons le fait que toute forme de profilage soit considérée comme un facteur de risque. Nous nous référons pour cela notamment au document de la CNIL recensant les opérations de traitement pour lesquelles une AIPD est requise[8]. Nous recommandons à la CNIL de revoir ce critère à l'aune des observations ci-dessus.

[8] Liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise https://www.cnil.fr/sites/cnil/files/atoms/files/liste-traitements-aipd-requise.pdf

C0.07	Nous considérons nécessaire d'introduire ici que le sous-traitant n'est pas tenu de fournir des informations confidentielles ou sensibles qui pourraient être utilisées de manière malveillante ou prédicable pour ce dernier. Il a en effet l'obligation de protéger ces informations et de ne les divulguer que dans les conditions prévues par le contrat ou la législation applicable. Il est aussi important de noter le fait que les données ne sont pas forcément cloisonnées et qu'il est notamment très rare de voir les PME mettre en place un cloisonnement du système d'information, la pratique étant que ce sont les fichiers contenant les données ou les bases de données qui sont séparés les un(e)s des autres. Nous recommandons à la CNIL de prendre en compte ce point afin de favoriser l'adoption de la certification par les plus petites entreprises. En outre, nous souhaiterions que la CNIL clarifie ce qui est attendu par l'exigence selon laquelle « le sous-traitant **doit disposer** d'une description générale… ». Cette description doit-elle être tenue à disposition uniquement à la demande de l'organisme de certification, ou s'agit-il d'un document devant être rendu public ? Si cette dernière option était retenue, il serait essentiel de garantir que le sous-traitant ne soit pas contraint de divulguer des informations confidentielles susceptibles d'être exploitées par des tiers à des fins malveillantes ou préjudiciables pour le sous-traitant (exemple : pour les prestataires intermédiaires). De la même manière, ce niveau de détail ne nous semble pas explicitement requis par l'article 28 du RGPD et pourrait donc imposer des charges supplémentaires aux sous-traitants[9].
C0.08	Ce critère nous semble très problématique. Tout d'abord, il ne repose sur aucune base légale ou réglementaire. Il s'agit donc d'une obligation supplémentaire au RGPD qui impose au sous-traitant de tenir un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement (article 32.2 du RGPD). En exigeant des sous-traitants qu'ils cartographient indépendamment les flux de données, cette obligation pourrait faire double emploi avec les efforts déjà déployés par les responsables du traitement et potentiellement outrepasser le rôle du sous-traitant tel que défini à l'article 28 du RGPD (qui se limite au traitement pour le compte du responsable du traitement). Deuxièmement, la définition d'un « flux » de données mériterait d'être clarifiée puisque celle-ci n'est pas définie dans le RGPD. Cela représente une difficulté supplémentaire pour les entreprises.

[9] Les responsables du traitement peuvent déjà évaluer l'adéquation des systèmes d'un sous-traitant par le biais d'audits techniques, d'accords contractuels ou d'analyses d'impact relatives à la protection des données. Exiger des divulgations supplémentaires lors de la certification risque de dupliquer ces efforts.

	Par ailleurs, aucune indication n'est donnée ici sur le niveau de détail attendu renforçant les risques d'interprétation différenciée selon l'organisme de certification et aucune garantie de confidentialité (et ce malgré la sensibilité des informations potentiellement demandées) n'est apportée. Imposer la mise à disposition d'une cartographie recensant l'ensemble des flux de données dans le cadre de l'ensemble des traitements -selon le niveau de détail requis- pourrait être un travail démentiel pour les petites et moyennes entreprises. Peu d'entre elles pourraient être en mesure d'y parvenir. Enfin, à l'instar du C0.07, le « doit disposer » prête à confusion, a fortiori dans ce cadre qui nécessite des évolutions régulières. Nous recommandons à la CNIL d'adopter une approche de la sécurité fondée sur les risques permettant aux entreprises de conserver une flexibilité nécessaire à leurs activités et de s'en tenir strictement aux obligations et à la terminologie du RGPD afin de garantir une meilleure lisibilité et cohérence du référentiel. Cela permettrait de faciliter l'adoption de la certification en évitant toute complexification potentiellement dissuasive.
C0.09	Deux éléments principaux sur lesquels nous souhaitons revenir : - <u>Le projet de référentiel va au-delà du RGPD</u> : demander au sous-traitant d'identifier l'ensemble des obligations qui lui incombent ne repose à nouveau sur aucune base légale ou réglementaire et ajoute une incertitude supplémentaire quant à ce qui doit être considéré comme « dispositions législatives ou réglementaires en matière de protection des données »[10] ; - <u>Le critère n'a que peu d'intérêt, crée une charge importante et est insuffisamment précisé :</u> nous ne percevons pas l'intérêt pour les responsables de traitement d'obtenir ces informations de la part des sous-traitants. Une telle exigence semble ouvrir la porte à une extension injustifiée des obligations pesant sur ces derniers, les contraignant à justifier des aspects qui dépassent le cadre contractuel les liant aux responsables de traitement. De plus, l'absence de précision quant au niveau de détail requis laisse une marge d'interprétation trop large aux organismes de certification, créant ainsi une insécurité juridique pour les sous-traitants. Enfin, l'article ne précise pas si l'identification des exigences légales est une condition préalable à la certification ou simplement une obligation de divulgation. Nous recommandons à la CNIL d'exclure ce critère du projet.

[10] Exemples de l'article 226-16 du Code pénal ou de l'incertitude autour du concept de « droit national » (droit français ? droit de l'UE ?)

C0.09 bis	Ce critère est l'un des plus problématiques de l'ensemble du projet de référentiel d'évaluation et ce pour trois principales raisons : La première est qu'il place le sous-traitant dans une situation d'insécurité juridique considérable. Il ne peut, et ne pourra jamais, avoir une connaissance exhaustive des réglementations applicables à chacun de ses clients, ce qui ne relève ni de son rôle ni de sa responsabilité. En outre, cette exigence apparaît dénuée de toute pertinence dans le cadre de la relation contractuelle entre le sous-traitant et le responsable de traitement, dès lors que le Code civil consacre la notion de « bonne foi » comme un principe fondamental du droit des contrats[11]. Cette situation placerait par ailleurs le sous-traitant dans une situation de fragilité notamment vis-à-vis de ses clients étrangers. La deuxième est qu'il surinterprète le rôle du sous-traitant tel que prévu par les textes et renforce *de facto* sa responsabilité. Aucune disposition légale contraint le sous-traitant à connaître l'ensemble des réglementations « susceptibles » d'être applicables à son client. Le RGPD ne fixe au sous-traitant qu'une obligation d'information immédiate lorsque, selon lui, une instruction du responsable de traitement est non conforme[12]. La dernière correspond au rôle de conseil juridique que le critère semble accorder aux sous-traitants vis-à-vis des responsables de traitement. Les sous-traitants ne sont pas des avocats, ne font pas commerce de droit et ne doivent pas le faire. Il s'agit ici d'un critère dangereux qui pourrait contrevenir au monopole des avocats en matière de rédaction d'actes et de conseil juridique, notion centrale du droit, instaurée par la loi n° 71-1130 du 31 décembre 1971. Par ailleurs, imposer au sous-traitant d'« identifier les obligations qui nécessitent la mise en œuvre de mesures spécifiques de protection des données » pourrait le conduire à assumer le rôle de responsable de traitement ou de responsable conjoint du traitement. Nous recommandons à la CNIL de renoncer à ce critère.

Partie 1 : Les conditions de la sous-traitance – les engagements contractuels

Plan du référentiel	Commentaires Alliance Digitale

[11] Code civil, articles 1112 et suivants
[12] Article 28.3 RGPD

C1.01	L'exigence selon laquelle seuls les acteurs soumis au droit européen peuvent prétendre à la certification apparaît comme une restriction injustifiée. Nous nous interrogeons pourquoi une telle condition a été retenue, alors même qu'elle empêche de nombreux acteurs d'y accéder. Si la certification vise à constituer un atout, il semble contre-productif d'en restreindre l'accès à des pays comme la Suisse ou le Royaume-Uni par exemple. Par ailleurs, la définition de la juridiction compétente en cas de litige n'est pas un élément obligatoire du contrat. Nous recommandons à la CNIL de reconsidérer cette restriction territoriale.
C1.02	Plusieurs éléments sont à relever ici : - L'insertion au sein du b) des « données relative à des données de localisation telles que définies par la Directive 2002/58/CE » est injustifiée. Il ne s'agit ni d'une catégorie particulière de donnée au sens de l'article 9 du RGPD ni de données « hautement personnelles » ; - Les informations qui sont exigées pour le respect de ce critère ne sont pas nécessairement connues par le sous-traitant. Le sous-traitant n'est pas en mesure de savoir l'ensemble des données introduites par son client dans le cadre par exemple d'un service de stockage ; - Par ailleurs, le critère ne distingue pas ce qui constitue une obligation de ce qui relève d'une exigence facultative. Par exemple, l'obligation de d'inclure dans le détail des traitements réalisés pour le responsable de traitement les données sensibles au sens de l'article 9 du RGPD ne devrait s'appliquer que si le produit concerné est effectivement destiné à traiter de telles données. Dans le cas contraire, cette exigence devrait être facultative. Nous recommandons ici de : - Retirer la référence aux données de localisation ; - Mieux distinguer ce qui constitue une obligation applicable à tous les traitements de ce qui ne s'impose que dans des cas spécifiques en fonction de la nature du traitement pour lequel le sous-traitant candidate à la certification ; - Ajouter une clause permettant de prendre en compte la connaissance des informations par le sous-traitant en ajoutant par exemple une mention comme « si l'information est connue » ou « le cas échant ».
C1.03	Il est important ici de mentionner que la durée d'un traitement n'est pas nécessairement équivalente à la durée du contrat. Certains traitements peuvent s'étendre après la fin du contrat dans certains cas pour permettre les retours de performance d'une campagne publicitaire (exemples dans le cas de l'email

	marketing avec les emails non délivrés, les « NPIA » - N'habite Pas à l'Adresse Indiquée). Il est à noter que c'est au responsable du traitement de déterminer la durée de conservation des données, celle-ci constituant un moyen essentiel selon les lignes directrices 07/2020 du CEPD. En pratique, les clients peuvent instruire le sous-traitant de conserver les données personnelles au-delà de la durée initialement prévue, sans que cette prolongation ne soit disproportionnée, dès lors qu'elle reste nécessaire au regard des finalités spécifiques. Il en va de même pour la durée de conservation des données qui peut être bien plus longue, notamment afin de répondre aux demandes d'exercice des droits si cela est nécessaire.
C1.04	Le présent critère s'appuie sur l'article 28.3 du RGPD relatif aux obligations contractuelles des sous-traitants. Toutefois, sa lecture et compréhension sont rendues plus difficiles en raison d'une reformulation des obligations issues de cet article, ainsi que d'un renvoi à onze critères distincts du projet de référentiel, qui détaillent de manière plus spécifique ces exigences et dont nous comprenons qu'ils doivent, pour chacun d'entre eux, être également imposés dans le contrat. Cette approche risque surtout de complexifier, d'alourdir et de rallonger les démarches contractuelles entre les responsables de traitements et les sous-traitants. Nous recommandons ici à la CNIL de s'en tenir à la répétition de l'article 28.3 du RGPD qui est déjà suffisamment normé.
C1.05	Ici est fait mention pour la première fois de la « phase précontractuelle » et du « prospect ». Nous souhaiterions comprendre précisément ce à quoi la CNIL fait référence : - S'agit-il de la phase de négociation avec un prospect confirmé qui a donc accepté l'offre commercial du sous-traitant et avec lequel des négociations purement contractuelles sont en cours ou ; - Est-ce la phase de démarchage de plusieurs prospects à qui le sous-traitant présente une offre commerciale (exemple : phase d'appel d'offres) ? Dans la seconde hypothèse, aucune obligation du RGPD ne devrait pouvoir s'appliquer. En effet, le sous-traitant ne traite pas de données pour le compte et sur instruction d'un prospect mais uniquement pour le compte et sur instruction du responsable de traitement (aucun service n'étant effectué, aucun traitement de donnée personnelle n'est opéré). Par conséquent, dans une phase de démarchage, le prospect ne peut être considéré comme responsable de traitement car aucun traitement de données personnelles n'est opéré à ce stade. Par ailleurs, cette exigence va bien au-delà de l'article 28 du RGPD et des lignes

	directrices du CEPD 07/2020 au point 1.3.1 qui prévoient que l'accord entre un responsable du traitement et un sous-traitant inclut les instructions du responsable du traitement, y compris toute information sur les transferts vers des pays tiers ou des organisations internationales. En effet, ces informations sur les transferts de données en dehors de l'Union européenne ne s'appliquent pas à une relation entre un sous-traitant et un prospect, mais uniquement à un sous-traitant avec le responsable du traitement. Nous souhaiterions que la CNIL clarifie ici ce qui est entendu ici et ajuste la rédaction de ce critère en conséquence.
C1.06	Ce critère renvoie à deux observations principales : - Le risque de détournement qu'il implique : l'exigence de transparence sur la liste des prestataires avec lesquels ils travaillent expose le sous-traitant au risque de voir le prospect les solliciter directement et ainsi fragiliser, voire anéantir pour les prestataires intermédiaires, son modèle économique. Si cette éventualité est généralement encadrée lorsqu'un prospect devient client, notamment grâce à l'insertion de clauses de non-sollicitation dans les contrats, ces clauses ne peuvent pas être mises en place au stade de la prospection, laissant ainsi les sous-traitants sans protection face à un détournement potentiel de leurs partenaires ; - Les difficultés anticipées pour l'appliquer : le sous-traitant n'a pas forcément connaissance de la liste des partenaires impliqués dans une sous-traitance ultérieure avant de contractualiser avec le client. Par ailleurs, le présent critère semble difficilement applicable dans un contexte d'autorisation générale à la sous-traitance et semble à nouveau considérer que les traitements font nécessairement l'objet d'un transfert hors UE ; Cette obligation va au-delà de l'article 28.2 du RGPD qui indique que le sous-traitant ne peut faire appel à un sous-traitant ultérieur sans l'autorisation écrite préalable du responsable du traitement. En effet, ni le RGPD ni le CEPD ne précisent quelles informations le sous-traitant doit fournir concernant son sous-traitant ultérieur. Le projet de certification ne précise pas comment le processus d'évaluation prendra en compte cette exigence, notamment concernant la gestion des sous-traitants ultérieurs engagés après l'obtention de la certification Nous recommandons à la CNIL de renoncer à ce critère qui est difficilement applicable et risque de fragiliser le modèle économique de certains sous-traitants.
	Le projet de référentiel d'évaluation devrait donner plus de précisions sur le niveau de détail attendu concernant les mesures de sécurité notamment afin d'éviter des interprétations différentes selon l'organisme de certification. De la

C1.07	même manière, il serait opportun de renforcer ici la confidentialité des informations partagées par le sous-traitant dans la phase précontractuelle. Par ailleurs, l'obligation pour le sous-traitant de mettre à disposition des prospects la description synthétique du système d'information de sous-traitant et de la cartographie des flux est très difficile à mettre en œuvre. Au-delà de nos commentaires précédents sur les critères C0.07 et C0.08, il s'agit d'une obligation très lourde dans ce cadre et qui pose un problème de confidentialité majeur pour l'ensemble des sous-traitants. L'inclusion de déclarations d'applicabilité pour les mesures alternatives pose la question de la garantie que ces mesures sont correctement documentées, justifiées et évaluées quant à leur équivalence avec les mesures de sécurité standard. Cette exigence ne précise pas comment l'adéquation des mesures de sécurité sera évaluée lors de la certification et notamment s'il y aura des seuils pour la réévaluation obligatoire des mesures de sécurité (par exemple, lorsque les systèmes ou les opérations du sous-traitant subissent des changements importants). Nous recommandons à la CNIL ici de s'en tenir à l'obligation pour l'organisme de certification de vérifier qu'il y a une procédure en place sur les mesures de sécurité mais pas d'aller dans le détail de chacune d'entre elles. Autrement, la documentation à fournir serait trop importante pour le sous-traitant.
C1.09	Cette exigence va bien au-delà de la réglementation applicable car ni le RGPD ni le CEPD ne précisent que l'accord sur le traitement des données doit indiquer la procédure de traitement des demandes de droits sur les données. Bien que la répartition des rôles et les délais d'action du sous-traitant soient logiques et généralement déjà intégrés dans la plupart des accords, certaines difficultés peuvent survenir pour les sous-traitants ne disposant pas des ressources techniques nécessaires pour répondre aux demandes d'exercice des droits des personnes concernées. Nous considérons que ce critère devrait être revu pour plus de clarté et de précision. Les formulations nous paraissent en effet trop larges, risquant de générer des interprétations variables selon l'organisme de certification.
	Ce critère appelle certaines observations : - <u>Le critère n'est pas suffisamment protecteur</u> : le caractère inopiné du b) entraine une forte insécurité juridique pour les sous-traitants qui pourraient voir les audits se multiplier en même temps ; - <u>Il ne permet pas la flexibilité nécessaire entre les parties :</u> dans la pratique contractuelle, les audits ne doivent pas avoir lieu plus souvent que tous les 12 mois sauf en en cas de non-conformité relevée ou constatée ou dans le cadre d'un contrôle d'une autorité. Le critère ne reprend pas ses

C1.13	éléments et nous apparait donc insuffisamment protecteur du sous-traitant ; - Aucune indication n'est fournie concernant la définition d'un « intervalle raisonnable » ni sur l'entité responsable de sa détermination. Nous tenons à souligner que si cette responsabilité incombe aux organismes de certification, cela pourrait poser deux problèmes principaux : o Absence de base légale : ils ne disposent pas de l'autorité juridique pour définir de tels intervalles ; o Risque de divergences : sans directives claires, chaque organisme pourrait interpréter différemment la notion d'« intervalle raisonnable », entraînant une incohérence dans les pratiques de certification. Nous recommandons ici de prendre en compte la pratique du marché et l'intérêt des deux parties : - Leur permettant de définir une fréquence raisonnable pour ce type d'audit (exemple : 12 mois) ; - En autorisant le sous-traitant à faire valoir à son client un audit réalisé sur un périmètre similaire (par exemple : pour un autre client), dans une période raisonnable (12 mois ici aussi à titre d'exemple), avec la possibilité pour ce dernier de contester l'audit le cas échéant.
C1.14	Ce critère de documentation de la conformité entraine plusieurs problématiques : - Il ne se réfère pas au RGPD ni à aucune autre base légale. La CNIL n'a par ailleurs jamais fourni un modèle de documentation de cette nature et a parfaitement connaissance qu'aucune attestation permettant d'affirmer la conformité au RGPD n'existe. Cela viendrait compliquer la relation contractuelle en plaçant le sous-traitant dans une posture délicate qui pourrait être assortie de l'introduction de pénalités dans le contrat ; - Il emporte des problématiques de confidentialité importantes puisqu'aucune condition d'accès ou de restriction n'est précisée pour le client ou les sous-traitants du prospect. Le risque en matière concurrentiel est également important. Nous recommandons à la CNIL de retirer ce critère qui dissuade de candidater à l'obtention de la présente certification.
	Ce critère appelle plusieurs remarques : - La procédure de recueil des instructions ne repose là aussi sur aucune base légale et entraine un niveau de bureaucratisation pour les sous-traitants qui nous parait particulièrement important, notamment pour les petites entreprises ;

C1.15	- Le critère semble faire à nouveau du sous-traitant le conseil juridique du responsable de traitement notamment dans le cadre du d). Le RGPD se limite à une obligation d'information du sous-traitant et n'impose aucune une obligation de conseil ou d'analyse systématique et obligatoire de la légalité des instructions du responsable de traitement[13]. Cette obligation vient donc renforcer la charge pour le sous-traitant de façon dangereuse puisque ce dernier pourrait dès lors être tenu responsable dans ce cadre, brouillant par conséquent la frontière entre responsable de traitement conjoint et sous-traitant ; - Par ailleurs, le b) ne fait pas référence aux instructions, il n'a donc pas de lien avec le critère C1.15. En outre le e) concernant les « évolutions « et les obligations qui en découlent n'est pas suffisamment compréhensible et pourrait imposer un formalisme important et inutile. De plus, il n'existe pas de définition claire de ce qu'est une « évolution » du traitement. Le terme est assez vague et pourrait tout englober, d'un changement mineur à une modification substantielle des activités de traitement. Cela pourrait entraîner des désaccords entre les parties sur ce qui constitue une « évolution » nécessitant une notification. Nous recommandons à la CNIL de renoncer à ce critère ou à tout le moins à l'obligation d'analyse légale des instructions qui ne repose sur aucun fondement juridique et qui contrevient au monopole des avocats sur le conseil juridique, comme expliqué dans le commentaire du critère C0.09.
C1.15 bis	Plusieurs éléments : - <u>Aucune référence légale ne justifie cette exigence</u> : à l'instar de ce qui est écrit pour le critère précédent, ni le RGPD, ni aucun autre texte légal n'établit pas cette procédure ; - <u>Le critère semble contrevenir aux lignes directrices du CEPD sur les notions de responsable de traitement et de sous-traitant</u> : ces dernières précisant en effet qu'un client dans le cas d'une offre standardisée est considéré comme responsable de traitement lorsqu'il (1) choisit de recourir à un service et un prestataire et (2) que le prestataire ne traite pas les données personnelles à ses propres fins[14] ; - <u>Il brouille également la frontière entre responsable de traitement et sous-traitant :</u> il s'agit spécifiquement de l'obligation qui est lui est faite dans le

[13] Article 28.h RGPD : « informe immédiatement le responsable du traitement si, selon lui, une instruction constitue une violation du présent règlement ou d'autres dispositions du droit de l'Union ou du droit des États membres relatives à la protection des données »

[14] Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, Juillet 2020, Voir exemple p. 15, exemple du « service standardisé de stockage en nuage » https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_fr.pdf

	d) concernant l'aide à documenter les instructions, impliquant quasiment une obligation de configuration du sous-traitant pour le compte du client. Nous recommandons à la CNIL de renoncer à ce critère ou à restreindre l'obligation à la transparence concernant les options de paramétrage disponibles de l'offre de service existante, pendant toute la durée du contrat entre le sous-traitant et le responsable du traitement, afin de permettre l'évolution des services proposés par le sous-traitant.
C1.16	Ce critère est, à l'instar du C0.05, décorrélé de l'objectif et du périmètre de son projet de référentiel d'évaluation. Il peut en outre créer un déséquilibre dans la relation entre le responsable du traitement et le sous-traitant, ce dernier se retrouvant soumis à des décisions arbitraires de la part du responsable du traitement, en particulier en cas de désaccord sur la nécessité ou la légalité d'activités ultérieures de traitement. Par ailleurs, plusieurs éléments posent question : - Il est difficile de déterminer dans le a) ce à quoi le « test de compatibilité » fait référence, ni même ce qui est visé par l'« autorisation écrite » (le contrat ?). Cela nous semble renforcer la complexité du processus de façon inutile ; - Aucune mention n'est faite en cas d'évolution de la loi et les obligations qui en découleraient, notamment d'un point de vue contractuel. Nous considérons que la CNIL pourrait simplement faire un rappel à l'article 6.4 du RGPD pour simplifier cette partie.
C1.17	Ce critère est l'un des plus dissuasifs et problématiques du projet de référentiel d'évaluation. Le retrait de la certification ne saurait, par principe, entraîner l'illégalité des traitements concernés et conduire à leur suspension. Une telle disposition introduirait une insécurité juridique majeure pour les sous-traitants et nuirait gravement à leur réputation. En outre, aucune précision n'est apportée quant à la date de prise d'effet de la suspension et aussi aux conséquences de la suspension des traitements sur les engagements financiers ou encore sur le sort des prestations contractées mais non concernées par cette dernière. Dans ces conditions, la certification perdrait tout attrait pour les acteurs du marché. Par ailleurs, cette exigence dépasse une nouvelle fois le cadre du RGPD. En effet, l'article 42.7 du texte prévoit uniquement le retrait de la certification lorsque les exigences applicables ne sont plus satisfaites, sans faire mention d'une suspension des traitements. Enfin, il est important de noter qu'une modification législative peut entraîner des ajustements nécessaires des traitements de données pour maintenir la

	conformité légale. Si ces modifications n'ont pas été intégrées au processus de certification, le sous-traitant reste conforme aux exigences du RGPD, mais sa certification n'est plus à jour. Cette situation pourrait créer une divergence entre la conformité effective du traitement et la validité de la certification associée. Nous recommandons ainsi à la CNIL de renoncer à cette disposition et, concernant le retrait de la certification, d'apporter une interprétation plus précise de l'article 42.7 afin d'assurer une application plus souple et compréhensible pour les acteurs concernés.

Partie 2 : L'environnement de la sous-traitance – la préparation du traitement

Plan du référentiel	Commentaires Alliance Digitale
C2.01	Nous tenons à souligner que ce critère impose un niveau de traçabilité excessif, conduisant à une bureaucratisation disproportionnée pour les sous-traitants dépassant le cadre de l'article 28 du RGPD. Plus spécifiquement : - Le d) n'est pas forcément pertinent, notamment pour des prestations de type grand public comme l'hébergement des contenus par une plateforme ; - Idem pour le e) où ces informations ne sont pas forcément connues car les prestations ne nécessitent pas toujours ces informations sur les clients ; - Il en va de même pour les f) g) qui ne sont pas forcément à disposition du sous-traitant ou pour le h) puisque le sous-traitant n'est pas obligé de recourir à un sous-traitant ultérieur. Enfin, le f) fait référence à une donnée de nature "hautement personnelle", qui n'est pas un terme défini par le RGPD ou par une autre législation applicable. Par conséquent, nous recommandons de s'en tenir aux termes expressément définis par le RGPD afin notamment d'éviter toute interprétation contradictoire ou surinterprétation des dispositions légales et réglementaires applicables. Nous recommandons ici de s'en tenir aux éléments mentionnés par l'article 30.2 du RGPD.
	Les informations requises dans ce critère renvoient au critère précédent et excèdent les obligations de documentation définies par l'article 28 du RGPD. D'un point de vue opérationnel, le sous-traitant ne dispose pas toujours des informations demandées au moment du démarrage du traitement. Par exemple,

C2.02	dans le cadre d'une campagne publicitaire, le sous-traitant de l'annonceur peut ne pas avoir de date de fin prédéfinie, le traitement reposant sur d'autres critères tels que l'atteinte des objectifs fixés. Nous recommandons donc de s'en tenir aux exigences du registre des traitements prévues par l'article 28 du RGPD afin d'éviter une surcharge documentaire excessive et peu adaptée aux réalités opérationnelles des sous-traitants.
C2.03	L'obligation de désigner un délégué à la protection des données dépasse également le cadre de l'article 37 du RGPD. Si nous comprenons théoriquement cette exigence, nous considérons que la nomination d'un DPO et d'un « référent certification » (C2.05) le cas échéant, pourrait être perçue comme désincitatif pour les plus petites entreprises au regard des coûts associés.
C2.05	Le « référent certificateur » prévu par ce critère ajoute encore une complexité supplémentaire et surtout, un coût plus important. La création de ce nouveau rôle pourrait également être considérée comme incompatible avec l'approche du RGPD en matière de conformité, qui vise à établir un ensemble clair d'obligations pour les responsables du traitement et les sous-traitants, le DPO jouant un rôle central. L'ajout d'un rôle de « référent certificateur » sans base légale claire dans le cadre du RGPD pourrait compliquer à l'excès le cadre réglementaire et créer une ambiguïté juridique quant à la personne qui porte la charge ultime de la conformité en matière de protection des données. Si le projet semble encourager le cumul de cette fonction avec celle de DPO, il est important de noter que, notamment pour les entreprises faisant appel à un DPO externe, cela entrainera un autre coût supplémentaire pour elle lié à la certification. Enfin, la question de savoir qui définit ce qui constitue un « conflit d'intérêts » dans ce cadre reste floue. Une clarification est nécessaire sur les critères utilisés pour évaluer cette situation et l'ajout d'exemples pourrait être pertinent.
C2.07	Il est important d'exclure clairement du champ d'application de ce point les transferts de données vers les pays bénéficiant d'une décision d'adéquation de la part de la Commission européenne, ainsi que vers les membres de l'Espace économique européen (EEE) qui ne font pas partie de l'Union européenne (UE). S'agissant des « mesures supplémentaires », nous nous demandons lorsque le responsable de traitement (RT) instruit son sous-traitant (ST) de transférer des données personnelles à un autre sous-traitant du RT ou à un autre RT ou RT conjoint, qui est responsable de l'analyse du cadre juridique applicable et de la mise en place des mesures de protection supplémentaires ? En outre, le RGPD n'impose pas au sous-traitant de s'assurer que l'importateur de données a accompli les formalités nécessaires dans le pays où il est établi (C2.06), d'identifier si la législation et les pratiques du pays de destination sont

	susceptibles de compromettre l'efficacité des garanties fournies par l'outil de transfert choisi, ni d'identifier et de documenter des mesures supplémentaires pour assurer un niveau équivalent de protection des données (C2.07).
C2.09	Ici, nous souhaitons que la CNIL clarifie le périmètre de ce critère et le limite aux sous-traitants d'un traitement certifié. Il est important de noter que l'obligation d'informer les prospects sur les sous-traitants ultérieurs et leurs activités de traitement connexes est très contraignante, en particulier dans les secteurs où les relations du sous-traitant avec les sous-traitants ultérieurs peuvent évoluer ou changer fréquemment. Nous demandons également à la CNIL de renoncer au délai 1 mois qui est prévu par ledit critère pour soumettre la demande d'autorisation ou informer le client du sous-traitant concernant le recrutement d'un sous-traitant ultérieur après la signature du contrat. Nous considérons trois raisons principales : - Le RGPD ne prévoit pas de délai et renvoie à la liberté contractuelle des parties. A noter que cette liberté contractuelle est prévue par la Commission européenne dans ses clauses contractuelles types responsable de traitement sous-traitant, en laissant un champ à compléter par les parties au sein de l'article 7.7 desdites clauses[15] ; - Le délai est trop rigide et ne permet pas de s'adapter aux différentes situations envisageables ; - Il peut être enfin complexe opérationnellement pour certaines prestations, par exemple, lorsqu'il s'agit de faire appel à une multitude sous-traitants ou de tester plusieurs sous-traitants pour assurer la meilleure performance possible.
C2.11	Même commentaire concernant le périmètre que le critère C2.09. Nous alertons la CNIL sur la difficulté de la lecture avec les renvois nombreux (30 sur l'ensemble de ce critère) à d'autres critères du projet de référentiel et la documentation importante (et donc le coût associé) qui est requise. Les mesures de sécurité minimales, listées par la CNIL, à mettre en œuvre par le sous-traitant nous paraissent inappropriées : - Le paysage de la sécurité évolue rapidement, et imposer un ensemble fixe de mesures de sécurité pourrait conduire à des protections obsolètes ou inadéquates au fil du temps. Les sous-traitants peuvent avoir besoin de mesures différentes ou plus avancées en fonction de la nature du traitement ; - La CNIL exige des « mesures d'anonymisation des données » (critère C32.20), mais toutes les activités de traitement ne nécessitent pas d'anonymisation. Pour certains services, la pseudonymisation ou le cryptage peuvent être plus appropriés. De même, les « mesures

[15] Article 7.7 https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32021D0915

	d'exportation des données » (critère C32.21) peuvent ne pas être nécessaires pour les sous-traitants qui ne transfèrent pas de données en dehors d'un environnement contrôlé ; - Cela peut conduire à une « conformité par case à cocher », les entreprises se concentrant sur le remplissage de documents au lieu de mener des évaluations significatives des risques de sécurité adaptées à leurs menaces réelles ; - Cela imposerait une lourde charge de conformité pesant sur les sous-traitants, qui doivent non seulement documenter les mesures de sécurité imposées par le RGPD, mais aussi toutes les mesures de sécurité supplémentaires requises par d'autres lois (critère C0.09), ainsi que les mesures de sécurité pour les transferts de données spécifiques, les instructions de traitement et les configurations de services ; - Le projet de référentiel de certification ne distingue pas entre les traitements à faible et à haut risque, imposant à chaque sous-traitant de documenter les mêmes mesures de sécurité étendues. Enfin, de nombreuses entreprises suivent déjà les meilleures pratiques et certifications en matière de sécurité (par exemple, ISO 27001, SOC 2, etc.). Le cadre de la CNIL ne précise pas si le respect de ces normes pourrait permettre de remplir ces obligations, ce qui entraînerait un risque de duplication des audits de sécurité et des efforts de documentation. Nous souhaiterions que la CNIL revoit ce critère à l'aune des éléments ci-dessus.
C2.12	Nous alertons ici également sur la lourdeur administrative et financière du respect de ce critère. Au lieu de se concentrer sur les risques réels en matière de sécurité, les entreprises risquent de consacrer des ressources excessives à justifier les écarts par rapport à une liste rigide de mesures. Par ailleurs, il serait opportun que le projet clarifie les conséquences du non-respect de l'échéance mentionnée au d).
C2.13	Le point b) introduit une nouvelle obligation qui n'est pas explicitement prévue par le RGPD. En effet, tous les traitements certifiés ne présentent pas nécessairement un risque élevé justifiant la réalisation d'une analyse d'impact relative à la protection des données (AIPD). De plus, aucune précision n'est apportée quant à la situation où les critères définis à l'article 35 du RGPD ne seraient pas remplis et aucune protection du sous-traitant n'est envisagée concernant la mise à disposition de ces informations à leurs clients.

	La formulation « susceptible de tenir à disposition » nous apparait par ailleurs maladroite. Cela veut-il dire que ces éléments sont facultatifs ? Nous demandons à la CNIL de retirer l'obligation de tenir à disposition des éléments d'analyse d'impact relative à la protection des données et de tenir compte du niveau risque du traitement.
C2.14	Nous nous interrogeons ici sur la portée du « lorsque ». S'agit-il dès lors d'un critère facultatif pour l'obtention de la certification ? L'utilisation des termes « probabilité d'événement » et « gravité des conséquences » dans le c) soulève des interrogations. En effet, l'analyse des risques, qui relève normalement de la responsabilité des responsables de traitement (RT), semble ici transférée à celle des sous-traitants (ST) qui ne disposent pas toujours des informations qui permettent d'évaluer la « gravité » des conséquences d'un évènement. Cette situation est problématique, car les éléments nécessaires à une telle évaluation dépendent largement des spécificités du client. Bien que l'intention soit louable, cette démarche paraît disproportionnée par rapport aux exigences du RGPD et de l'article 28.3, qui requiert seulement une assistance en matière de sécurité, plutôt qu'un cadre complet de gestion des risques pour chaque traitement. Il est donc important que la CNIL reconsidère cette exigence.
C2.15	Nous formulons la même remarque quant à ce critère s'agissant du « lorsque ». Par ailleurs, plusieurs éléments devraient être reconsidérés : - Une AIPD ne peut avoir lieu à la demande du client ou s'adapter aux hypothèses du client comme l'indiquent les a) et b). Le sous-traitant (ST) a l'obligation d'aider le responsable du traitement (RT) à réaliser une analyse d'impact relative à la protection des données (AIPD), mais il n'est pas tenu de la réaliser à sa place. Une opération de traitement effectuée par le ST peut constituer une partie du traitement entrepris par le RT. L'AIPD s'applique à un traitement dans son ensemble et non à une opération spécifique au sein de ce traitement. Par conséquent, seul le RT est en mesure d'évaluer la nécessité d'une AIPD, car il connaît l'intégralité du traitement concerné ; - Le sous-traitant ne définit ni les finalités du traitement, ni son fondement comme cela est mentionné dans le c) ; - Enfin, les 5 premières obligations listées dans le d) sont en dehors des compétences et du rôle du sous-traitant[16].

[16] Les lignes directrices WP 248 du groupe de travail Article 29 précisent bien que le sous-traitant doit aider le responsable du traitement à réaliser l'AIPD et lui fournir toutes les informations nécessaires. https://www.cnil.fr/sites/cnil/files/atoms/files/wp248_rev.01_fr.pdf

	Nous souhaiterions que la CNIL accepte d'adapter la rédaction de ce critère en conséquence.
C2.16	L'article 39 du RGPD ne confie pas la mission au DPO de détecter les incidents de sécurité comme indiqué dans le a). Ce point devrait être retiré d'autant plus que la procédure est très couteuse et nécessite un fort niveau de maturité pour être mené à bien. Par ailleurs, le RGPD ne demande pas aux sous-traitants de juger si un incident de sécurité constitue une violation de données à caractère personnel. Avec ce critère C2.16, la CNIL impose un processus décisionnel pour l'arrêt des opérations de traitement (critère C32.19). Néanmoins, cette exigence dépasse les obligations du RGPD, qui ne requièrent pas des sous-traitants qu'ils interrompent les opérations, à moins qu'une disposition contractuelle ne le stipule. Cela pourrait compromettre la continuité des activités sans l'implication du responsable du traitement.
C2.17	Ici, il est important de noter que ce qui est demandé du a) au e) n'est pas toujours possible pour le sous-traitant. A titre d'exemple, l'hébergeur des données personnelles peut ne pas avoir accès à ces données permettant l'identification des informations concernées par la demande de la personne concernée. Cela peut poser des problèmes, notamment en ce qui concerne la capacité de l'hébergeur à répondre aux demandes d'accès ou de rectification, si les données nécessaires à l'identification ne sont pas directement accessibles. Il en va de même pour l'obligation de fournir, même « à défaut », une « interface de gestion des demandes d'exercice des droits », qui incombe au responsable de traitement dans le RGPD, sauf si cette tâche relève d'une instruction donnée par celui-ci dans le cadre du contrat avec le sous-traitant. Nous recommandons à la CNIL de revoir ce critère à l'aune de ces observations.

Partie 3 : La réalisation de la sous-traitance – la mise en œuvre du traitement

Plan du référentiel	Commentaires Alliance Digitale
C3.01	Nous ne comprenons pas pourquoi le contenu des instructions provenant du responsable de traitement sont incluses dans le projet de référentiel concernant les sous-traitants. Plus spécifiquement : - Concernant les catégories de destinataires du c), le RGPD ne mentionne pas cette obligation, même dans l'article 28 dédié aux sous-traitants, ni dans les lignes directrices du CEPD concernant la notion de responsable de traitement et sous-traitant ;

	- Le d) nous semble contraire à ses mêmes lignes directrices qui prévoient expressément que les mesures de sécurité relèvent des moyens non essentiels[17] ; - Nous considérons que le f) correspond à une généralité inutile en l'espèce. Il serait préférable de préciser qu'il s'agit de la validation des informations par le responsable de traitement, qui est seul responsable du contenu de ces informations. Nous demandons à la CNIL de prendre en compte l'ensemble des points exposés ci-dessus.
C3.02	Ce critère nous parait problématique. Tout d'abord, il rend le sous-traitant responsable de la sécurité des données personnelles dès le démarrage du traitement mais le rend dépendant des instructions du responsable de traitement. Cela pose un problème important et va à l'encontre de l'objectif de sécurité juridique. Par exemple : que faire si les instructions du RT sont légales mais vont à l'encontre des exigences du référentiel de certification que le sous-traitant souhaite obtenir ? Ou si les évolutions demandées par le responsable de traitement vont dans un sens moins protecteur ? Par ailleurs, le sous-traitant semblerait tenu de confirmer régulièrement au responsable de traitement le maintien des mesures de sécurité, au minimum une fois par an. Si cette interprétation est correcte, une telle exigence nous paraît injustifiée et lourde. Nous recommandons à la CNIL de faire évoluer ce critère.
C3.03	Nous considérons qu'il serait opportun ici d'adresser la question du partage de la charge financière. Nous souhaiterions éviter que la certification entraine une complexité accrue entre les parties à ce niveau-là. En l'espèce, les coûts associés à l'évolution des instructions du responsable de traitement devrait lui revenir. Par ailleurs, le d) ne nous semble pas suffisamment précis quant à la détermination de la répartition des obligations entre le responsable de traitement et le sous-traitant. Par exemple : si le transfert résulte du choix d'un sous-traitant ultérieur par le responsable de traitement, qui est responsable de l'analyse du transfert (évaluation des risques, mise en place des mesures techniques et

[17] Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, Juillet 2020, Voir point 40 page 17 » https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_fr.pdf

	opérationnelles, etc.) ? De la même manière, que se passe-t-il en cas d'invalidation de l'accord d'adéquation EU-US ? Enfin, cette obligation ne repose sur aucun fondement juridique et ne provient pas non plus d'une interprétation du CEPD dans ses lignes directrices.
C3.04	Cette proposition pourrait s'avérer trop exigeante pour les sous-traitants si la notion d'« interface de gestion » n'est pas clairement définie ou si sa mise en œuvre requiert des ressources opérationnelles importantes. Par exemple, en cas de volume élevé de demandes, les sous-traitants pourraient être confrontés à une charge importante pour y répondre rapidement. De plus, la CNIL pourrait-elle préciser la différence de ce critère avec le C2.17 ?
C3.06	Ce critère entraine une lourdeur administrative et technique difficile à mettre en œuvre et ne repose pas sur l'interprétation que nous avons du RGPD. Ledit critère est par ailleurs particulièrement peu flexible et ne laisse aucune marge de manœuvre au sous-traitant. Il en va de même pour les critères suivants liés aux obligations de formation. Par exemple, le critère revient à obliger le sous-traitant à former l'ensemble de ses salariés puisque théoriquement, tous peuvent être une « source de risque humaine potentielle » ou a minima avoir « une tâche en lien avec les traitements recensés » (C3.07 a)). Cela nous paraît là-aussi une disposition très couteuse. Par ailleurs, il impose un délai d'un an pour les sessions de sensibilisation et les tests de compréhension. Celui-ci ne repose sur aucune base légale ou pratique opérationnelle et peut être préjudiciable pour le sous-traitant. Enfin, nous considérons que la Charte informatique mentionnée n'est pas le document applicable aux règles de sécurité spécifiques aux traitements des données en tant que sous-traitant. Elle devrait donc être retirée. Nous recommandons à la CNIL de laisser plus de marge de manœuvre au sous-traitant quant à la formation de ses salariés et de prévoir une exception si le dépassement du délai mentionné au b) et c) est dûment justifié par le sous-traitant.
C3.07	Mêmes remarques ici concernant le formalisme exacerbé (qui va même jusqu'à décrire le contenu des formations), le coût pour les entreprises et notamment les TPE/PME (qui n'ont pas vocation à devenir des centres de formation) et les délais imposés pour le programme de formation. Nous considérons que l'organisme de certification devrait avoir accès aux différentes étapes du processus de formation et à leur organisation dans les grandes lignes mais qu'il n'est pas nécessaire ni souhaitable qu'il obtienne autant d'information.

C3.08	A nouveau, ici nous contestons le formalisme demandé qui s'aventure même dans les contrats de travail avec l'obligation non seulement d'ajouter une « clause de confidentialité spécifique » (qui n'existe pas dans le RGPD) mais également qui définit les engagements qu'elle doit contenir. L'entreprise n'a plus aucune marge de manœuvre. Nous considérons que ce point devrait être retiré.
C3.09	Ce critère est dissuasif pour les TPE/PME et risque de les décourager à candidater à la certification pour les raisons suivantes : - Certains rôles nécessitent des mises à jour plus fréquentes (par exemple, les équipes de sécurité informatique qui gèrent des traitements à haut risque) ; - D'autres peuvent ne pas nécessiter de mises à jour annuelles (par exemple, le personnel administratif ayant un accès limité aux données) ; - Une approche fondée sur les risques serait plus conforme aux principes de proportionnalité et de nécessité du RGPD. Les mises à jour annuelles pourraient également ne pas toujours être nécessaires : - Certaines activités de traitement restent inchangées pendant des années. Le RGPD n'impose pas de cycle de mise à jour fixe ; - Les mises à jour doivent être déclenchées par des changements importants, et non par une règle basée sur le temps.
C3.10	Ce critère impose un registre des « incidents de sécurité ». Le RGPD définit et encadre les violations de données personnelles (abordées dans le critère suivant) et non les « incidents ». Cela peut avoir une portée très générale et entrainer une situation sous-optimale où le sous-traitant serait contraint de partager ces « incidents » aux clients même lorsqu'ils ne les impactent pas. Nous recommandons ainsi à la CNIL de renoncer à ce critère.
C3.11	Ce critère dépasse le cadre légal de l'article 33.4 du RGPD. Il est indiqué dans le critère que « *Si le Sous-traitant n'est pas en mesure de fournir toutes ces informations en même temps, il* ***doit notifier*** *à son client la violation de données dès qu'elle est établie en lui fournissant les informations disponibles à ce moment-là* » alors que l'article sur lequel il repose dispose que : « *Si, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, les informations* ***peuvent être*** *communiquées de manière échelonnée sans autre retard indu* » Nous recommandons à la CNIL de ne pas dépasser le cadre légal ici.
	Nous considérons ici que la périodicité imposée pour réaliser un audit technique du système d'information de sous-traitance (« a minima tous les ans ») est trop exigeante et ne correspond pas aux réalités du marché.

C3.12	Par ailleurs, le RGPD n'exige pas explicitement des audits annuels, il impose seulement que les mesures de sécurité soient « régulièrement testées ». Certains sous-traitants pourraient également ne pas avoir besoin d'un audit technique complet chaque année si leurs opérations de traitement restent inchangées. Au lieu d'exiger un audit technique complet chaque année, la CNIL pourrait autoriser une fréquence des audits basée sur les risques. Cela renforce le caractère dissuasif du projet de référentiel. Nous suggérons à la CNIL de l'adapter.

Partie 4 : La fin de la sous-traitance – l'arrêt du traitement

Plan du référentiel	Commentaires Alliance Digitale
C4.01	Nous considérons que ce n'est pas à la certification de prévoir le sort des données. Cette question doit être réglée contractuellement par les parties et ne devrait pas être un critère d'obtention de la certification. Par ailleurs les dispositions du présent critère ne nous semblent pas suffisamment adaptées aux réalités opérationnelles. Par exemple, la fin du contrat n'entraine pas nécessairement la destruction des données. Nous recommandons à la CNIL de renoncer à ce critère.
C4.02	Deux points principaux ici : - « L'authenticité de l'instruction » présent dans le a) est un concept qui nous parait difficile à comprendre et *a fortiori* à vérifier. Cela pourrait être utilement clarifié ; - Le c) n'est pas toujours applicable pour le sous-traitant, tout comme la restitution de la donnée dans un format structuré accompagné de la documentation explicative. Par exemple, les données peuvent être retournées sur des supports physiques.
C4.03	Que se passe-t-il lorsque la durée de conservation des données ne coïncide pas avec la durée de la prestation ? Le RGPD n'exige pas une correspondance stricte entre ces deux éléments, mais impose que la durée de conservation soit justifiée par la finalité du traitement et respecte le principe de minimisation. Une clarification sur ce point nous apparait nécessaire.
C4.04	Même remarque précédemment. Nous considérons globalement que la liste exhaustive exposée dans le critère risque de ne pas résister à l'épreuve du temps et d'être rapidement caduque.

	Par ailleurs les traces de journalisation du d) sont des données toujours nécessaires pour démontrer le respect des obligations de sécurité. Elles ne peuvent donc figurer ici. Enfin, le projet de référentiel d'évaluation omet de mentionner la destruction des supports physiques des données.
C4.06	Sur ce point, que se passe-t-il si les obligations légales de conservation des données mentionnées dans le c) évoluent ? La CNIL pourrait-elle préciser clairement ce qui est entendu par « délai de suppression automatique » dans le b) ? A quoi cela fait-il référence ? Enfin, la CNIL pourrait-elle aussi clarifier la phrase suivante : « Le Sous-traitant doit mettre à jour les informations relatives aux traitements qui sont nécessairement à l'actualisation du registre des traitements » ?

Partie 5 : L'amélioration du niveau de protection des données – les plans d'action

D'un point de vue général, il est important de noter que l'ensemble de cette partie nous apparait difficile à mettre en place compte-tenu des coûts associés, des équipes mis à contributions (DPO, RSSI etc.) et de la planification demandée. Nous estimons que cela renforce le caractère dissuasif de l'ensemble du projet.

Plan du référentiel	Commentaires Alliance Digitale
C5.01	Nous ne comprenons pas la planification à trois ans prévue par ce critère et le suivant. Nous considérons qu'elle n'a aucune base légale et réglementaire et que par ailleurs, elle ne prend pas en compte les contextes, tailles et risques des différentes entreprises (comme les PME). Nous recommandons à la CNIL de renoncer à ce délai.
C5.02	Même remarque que précédemment ici. S'agissant du e), il omet de mentionner les évolutions jurisprudentielles qui peuvent avoir un impact majeur également sur le plan d'évaluation des entreprises et ne prévoit pas le cas où le sort des données prévu soit la restitution. Enfin, s'agissant de l'obligation d'information du sous-traitant de « tout manquement d'un sous-traitant ultérieur à ses obligations contractuelles » : Comment établir l'existence d'un manquement ? Une simple accusation suffit-elle ou faut-il une décision juridique ou une reconnaissance formelle du manquement par le sous-traitant ultérieur ? Ce point soulève un risque important

	de conflit entre l'obligation de notification et le risque de diffamation, nécessitant une clarification sur les conditions de preuve et les responsabilités des parties prenantes.
C5.03	Ce critère est particulièrement inquiétant puisqu'il revient à déléguer une partie des réclamations des personnes concernées revenant légalement à la CNIL à l'organisme de certification. La CNIL est la seule autorité compétente pour recevoir et instruire des plaintes. L'organisme de certification n'a pas cette prérogative, ce qui peut induire une confusion chez les personnes concernées, qui pourraient croire à tort qu'une plainte déposée auprès de cet organisme équivaut à une saisine de la CNIL. Par ailleurs, quelles sanctions un organisme de certification serait-il habilité à prendre et sur quelle base (non-respect de la certification ou de la réglementation ?) ? Toute délégation de pouvoirs en ce sens ne serait pas conforme à la loi, nécessitant une clarification stricte des rôles et des compétences de chaque entité. Nous demandons à la CNIL de renoncer à ce critère.
C5.04	Ce critère ne repose sur aucun fondement juridiquement et mérite plus de précision. Par exemple, comment le sous-traitant est-il en mesure de justifier qu'il a mis en place une veille ? Devrait-il la faire parvenir au responsable de traitement ou à l'organisme de certification ? La CNIL pourrait-elle proposer ce service ?

Annexe I : Mesures de sécurité

Le projet de certification va bien au-delà du RGPD et de sa compétence lorsqu'il s'agit d'énumérer les mesures de sécurité qu'un sous-traitant doit prendre pour obtenir la certification.

La présente proposition semble ajouter un niveau de détail qui pourrait être en dehors de l'intention initiale du règlement, en particulier en ce qui concerne la gestion des clés cryptographiques, les mesures de journalisation et les exigences étendues en matière de contrôle d'accès. Ces exigences pourraient être considérées comme plus strictes que nécessaire pour les sous-traitants, étant donné que certains aspects de ces mesures de sécurité, tels que la gestion du chiffrement, pourraient être considérés comme relevant des responsabilités du responsable du traitement pour assurer la sécurité des données.

En particulier :

- Sur les processus de chiffrement : bien que l'importance du chiffrement soit reconnue dans le RGPD, prescrire des méthodologies détaillées (par exemple, la taille des clés de chiffrement ou des algorithmes de chiffrement spécifiques) pourrait imposer une charge excessive aux sous-traitants, en particulier à ceux qui disposent de ressources limitées. Le RGPD permet une certaine souplesse dans la mise en œuvre de mesures de sécurité

appropriées en fonction du contexte de traitement. L'approche de la CNIL risque d'imposer un modèle de sécurité unique ;

- Concernant le contrôle d'accès : bien que la journalisation et le contrôle d'accès soient des éléments standards et essentiels pour la sécurité, les sous-traitants ne sont pas toujours tenus d'être les seuls responsables de l'application et de la journalisation de chaque action de l'utilisateur ou de la surveillance de la communication de machine à machine. Ces responsabilités doivent être proportionnées et refléter le rôle et la responsabilité du sous-traitant dans la relation de traitement des données. Des exigences excessives en matière de journalisation et de surveillance pourraient être considérées comme une atteinte à la flexibilité opérationnelle des sous-traitants, en particulier dans les situations où le responsable du traitement devrait assumer davantage de responsabilités ;

- Concernant la sauvegarde, l'archivage et la récupération : on pourrait faire valoir que certaines responsabilités, telles que la gestion des plans de continuité des activités, conviennent mieux au responsable du traitement qui détient les données et contrôle l'ensemble des opérations de traitement des données. Le rôle du sous-traitant est de suivre les instructions du responsable du traitement de manière sécurisée, et non pas nécessairement de concevoir et de mettre en œuvre des systèmes complets de sauvegarde et de récupération, ce qui pourrait entraîner des coûts opérationnels inutiles pour les sous-traitants.

Plan du référentiel	Commentaires Alliance Digitale
C32.08	Nous estimons tout d'abord que le d) ne devrait pas être une obligation afin de ne pas dégrader la performance. S'agissant de la délégation à son client de l'authentification d'une partie des utilisateurs, nous comprenons qu'il s'agit des enjeux liés au single sign-on (SS0). Le cas échant, le client est responsable de la gestion de l'authentification de son côté, y compris pour son nom de domaine et tous les comptes associés. En cas de tentatives d'authentification suspectes ou incompatibles avec l'unicité des identifiants, il disposera des informations nécessaires pour les analyser. L'identification des utilisateurs autorisés et la gestion des accès relèvent donc de sa responsabilité. Nous recommandons d'adapter ce critère à l'aune de cette observation.
C32.09	Nous suggérons ici de renvoyer vers les recommandations relatives à l'authentification multi facteur et aux mots de passe de l'ANSSI[18].

[18] https://cyber.gouv.fr/publications/recommandations-relatives-lauthentification-multifacteur-et-aux-mots-de-passe

C32.10	De la même manière, il serait utile de renvoyer vers le référentiel général de sécurité de l'ANSSI ici[19].
C32.13	Idem, utile de renvoyer vers les recommandations sur le nomadisme numérique de l'ANSSI[20].
C32.16	S'agissant des mesures de journalisation et de la durée de conservation des données établie dans ce critère, elle dépend de la réglementation applicable et des sources de risque. Une durée « entre six mois et un an » ne devrait donc figurer ici.
C32.17	Nous suggérons ici de renvoyer vers les recommandations de sauvegarde des systèmes d'informations de l'ANSSI[21].
C32.25	Voir critère C0.06 : la charte informatique ne fait pas partie du cadre des politiques de sécurité du système d'information.

[19] https://cyber.gouv.fr/le-referentiel-general-de-securite-rgs
[20] https://cyber.gouv.fr/publications/recommandations-sur-le-nomadisme-numerique
[21] https://cyber.gouv.fr/publications/fondamentaux-sauvegarde-systemes-dinformation