Avis du comité (article 64)

Avis 3/2025 sur le projet de décision de l'autorité de contrôle française (AC FR) concernant les «critères de la certification "Lexing certification RGPD"»

Adopté le 8 avril 2025

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Table des matières

1 RÉSUMÉ DES FAITS 5
2 ÉVALUATION 5
3 CONCLUSIONS / RECOMMANDATIONS 11
4 OBSERVATIONS FINALES 13

Le comité européen de la protection des données

vu l'article 63, l'article 64, paragraphe 1, point c), et l'article 42 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (ci-après le «RGPD»),

vu l'accord sur l'Espace économique européen (ci-après l'«EEE») et, en particulier, son annexe XI et son protocole 37, tels que modifiés par la décision du Comité mixte de l'EEE nº 154/2018 du 6 juillet 2018[1],

vu l'article 64, paragraphe 1, point c), du RGPD et les articles 10 et 22 de son règlement intérieur,

considérant ce qui suit:

(1) Les États membres, les autorités de contrôle, le comité européen de la protection des données (ci-après l'«EDPB») et la Commission européenne encouragent, en particulier au niveau de l'Union, la mise en place de mécanismes de certification en matière de protection des données (ci-après dénommés «mécanismes de certification») et de labels et marques en matière de protection des données, aux fins de démontrer que les opérations de traitement effectuées par les responsables du traitement et les sous-traitants respectent le RGPD. Les besoins spécifiques des micro, petites et moyennes entreprises sont pris en considération[2]. En outre, la mise en place de certifications peut améliorer la transparence et permettre aux personnes concernées d'évaluer le niveau de protection des données offert par les produits et services en question[3].

(2) Les critères de certification font partie intégrante de tout mécanisme de certification. Par conséquent, le RGPD exige l'approbation des critères nationaux de certification d'un mécanisme de certification par l'autorité de contrôle compétente [article 42, paragraphe 5, et article 43, paragraphe 2, point b), du RGPD] ou, dans le cas d'un label européen de protection des données, par l'EDPB [article 42, paragraphe 5, et article 70, paragraphe 1, point o), du RGPD].

(3) Lorsqu'une autorité de contrôle a l'intention d'approuver une certification conformément à l'article 42, paragraphe 5, du RGPD, le rôle principal de l'EDPB est de garantir l'application cohérente du RGPD, au moyen du mécanisme de contrôle de la cohérence visé aux articles 63, 64 et 65 du RGPD. Dans ce cadre, conformément à l'article 64, paragraphe 1, point c), du RGPD, l'EDPB est tenu d'émettre un avis sur le projet de décision de l'autorité de contrôle approuvant les critères de certification.

(4) Le présent avis vise à garantir l'application cohérente du RGPD, notamment par les autorités de contrôle, les responsables du traitement et les sous-traitants, à la lumière des éléments essentiels que doivent contenir les mécanismes de certification. En particulier, l'évaluation de

[1] Les références aux «États membres» dans le présent avis doivent être comprises comme des références aux «États membres de l'EEE».
[2] Article 42, paragraphe 1, du RGPD.
[3] Considérant 100 du RGPD.

l'EDPB est effectuée sur la base des «lignes directrices 1/2018 relatives à la certification et à la définition des critères de certification conformément aux articles 42 et 43 du règlement» (ci-après les «lignes directrices») et de leur addendum fournissant des «orientations sur l'évaluation des critères de certification» (ci-après l'«addendum»).

(5) Par conséquent, l'EDPB reconnaît que chaque mécanisme de certification devrait être traité individuellement et est sans préjudice de l'évaluation de tout autre mécanisme de certification.

(6) Les mécanismes de certification devraient permettre aux responsables du traitement et aux sous-traitants de démontrer qu'ils respectent le RGPD; par conséquent, les critères de certification devraient refléter correctement les exigences et principes relatifs à la protection des données à caractère personnel énoncés dans le RGPD et contribuer à son application cohérente.

(7) Dans le même temps, les critères de certification devraient tenir compte d'autres normes et, le cas échéant, être interopérables avec celles-ci, telles que les normes ISO et les pratiques de certification.

(8) En conséquence, les certifications devraient apporter une valeur ajoutée à une organisation en contribuant à la mise en œuvre de mesures organisationnelles et techniques normalisées et spécifiées qui facilitent et améliorent de manière démontrable la conformité des opérations de traitement, en tenant compte des exigences sectorielles.

(9) L'EDPB salue les efforts consentis par les propriétaires de systèmes pour élaborer des mécanismes de certification, qui sont des outils pratiques et présentant potentiellement un bon rapport coût-efficacité, afin d'assurer une plus grande cohérence avec le RGPD et de favoriser le droit au respect de la vie privée et à la protection des données des personnes concernées en renforçant la transparence.

(10) L'EDPB rappelle que les certifications sont des outils de responsabilité volontaires et que l'adhésion à un mécanisme de certification ne réduit pas la responsabilité des responsables du traitement ou des sous-traitants en ce qui concerne le respect du RGPD ou n'empêche pas les autorités de contrôle d'exercer leurs missions et pouvoirs en application du RGPD et des législations nationales pertinentes.

(11) L'avis de l'EDPB est adopté conformément à l'article 64, paragraphe 1, point c), du RGPD, lu en combinaison avec l'article 10, paragraphe 2, du règlement intérieur du comité, dans un délai de huit semaines à compter du premier jour ouvrable après que le président du comité et l'autorité de contrôle compétente ont décidé que le dossier était complet. Sur décision du président, ce délai peut être prolongé de six semaines en fonction de la complexité de la question.

(12) L'avis de l'EDPB se concentre sur les critères de certification. Si l'EDPB a besoin d'informations de haut niveau sur les méthodes d'évaluation afin de pouvoir évaluer de manière approfondie l'auditabilité des projets de critères de certification dans le cadre de son avis, ce dernier n'inclut cependant aucune sorte d'approbation de méthodes d'évaluation en question.

A ADOPTÉ L'AVIS SUIVANT:

1 RÉSUMÉ DES FAITS

1. Conformément à l'article 42, paragraphe 5, du RGPD et aux lignes directrices, les «critères de la certification "Lexing certification RGPD"» (ci-après le «projet de critères de certification» ou les «critères de certification») ont été élaborés par Lexing, une entité juridique enregistrée en France (RCS PARIS 452 160 856) et soumis à l'autorité de contrôle française (ci-après l'«AC FR»).

2. L'AC FR a soumis son projet de décision approuvant les critères de certification et a demandé l'avis de l'EDPB conformément à l'article 64, paragraphe 1, point c), du RGPD le 30 janvier 2025. La décision relative au caractère complet du dossier a été prise le 26 février 2025.

3. La certification en question n'est pas une certification au sens de l'article 46, paragraphe 2, point f), du RGPD applicable aux transferts internationaux de données à caractère personnel, et elle ne fournit donc pas de garanties appropriées dans le cadre des transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales dans les conditions visées à l'article 46, paragraphe 2, point f). En effet, le transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale ne peut avoir lieu que si les dispositions du chapitre V du RGPD sont respectées.

2 ÉVALUATION

4. Le comité a procédé à son évaluation conformément à la structure prévue à l'annexe 2 des lignes directrices (ci-après l'«annexe») et à son addendum. Lorsque le présent avis reste muet sur une section spécifique des critères de certification, il convient de le lire comme le fait que le comité n'a pas d'observations et ne demande pas à l'AC FR de prendre des mesures supplémentaires.

2.1 REMARQUES GÉNÉRALES

5. Dans le cadre du projet de critère R05-S01-C01, le système introduit une classification des types de données à caractère personnel en cinq catégories. L'EDPB fait observer que, bien qu'une telle classification puisse effectivement faciliter l'évaluation globale des risques[4], une évaluation correcte devrait également prendre en considération d'autres facteurs que les types de données à caractère personnel, tels que la nature, la portée, le contexte et les finalités du traitement.

6. Le comité se félicite de l'inclusion de la section 1 «Exigences relatives aux engagements de la direction générale dans le domaine de la protection des données» dans le projet de critères de certification. Le comité note que le projet de critère R01-S01-C01 relatif aux orientations pour l'application de la législation en matière de protection des données prévoit que «si des orientations substantielles sont mises à jour, une nouvelle

[4] Voir les lignes directrices du groupe de travail «Article 29» concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679 du 4 avril 2017, WP248 rev.01, approuvées par l'EDPB le 25 mai 2018, p. 9 et 10.

communication est envoyée avant la fin de la période de trois ans dans un délai d'un mois à compter de la mise à jour». Dans ce contexte, le comité relève que le terme «substantiel» peut être assez large, entraîner une ambiguïté et entraver l'auditabilité de ce critère. À cette fin, le comité encourage l'AC FR à exiger du propriétaire du système qu'il précise quelles orientations sont «substantielles» (par exemple, en fournissant quelques exemples de ces orientations).

7. Le comité prend note de l'approche adoptée et décrite au point «1. Vue d'ensemble» dans les critères de certification. Le comité observe également que certains critères renvoient aux dispositions pertinentes du RGPD auxquelles ils visent à démontrer la conformité[5], et que l'annexe 5 consiste en un «tableau de concordance entre les obligations du RGPD et les critères du système». Toutefois, les références aux dispositions applicables du RGPD dans les critères ne sont pas systématiques et l'annexe 5 n'est pas exhaustive[6]. Le comité rappelle que, conformément aux «exigences générales» prévues à l'annexe 2 des lignes directrices 1/2018, toutes les références normatives doivent être indiquées. Par conséquent, le comité recommande à l'AC FR d'exiger du propriétaire du système qu'il renforce la granularité de l'annexe 5 en fournissant des précisions supplémentaires sur la correspondance entre les dispositions du RGPD et les critères de certification, afin de déterminer facilement les critères permettant à un demandeur de démontrer la conformité avec le RGPD. À titre subsidiaire, le comité recommande à l'AC FR d'exiger du propriétaire du système qu'il fasse référence à la disposition pertinente du RGPD pour chaque critère dans l'ensemble du document relatif aux critères de certification.

8. Le comité observe que le propriétaire du système définit le terme «anonymisation»[7] à l'annexe 4 des critères de certification. Compte tenu du fait que la notion d'anonymisation n'est pas explicitement définie dans le RGPD, l'EDPB encourage l'autorité de contrôle compétente à exiger du propriétaire du système qu'il examine si une telle définition est nécessaire. Si une définition du terme «anonymisation» est jugée nécessaire, l'EDPB recommande à l'autorité de contrôle compétente d'exiger du propriétaire du système qu'il veille à ce que le terme soit défini conformément au considérant 26 du RGPD[8].

2.2 BASE JURIDIQUE — CONSENTEMENT

9. En ce qui concerne le consentement des enfants, le comité note que, dans le projet de critère R06-S03-C02 «Conditions spécifiques du consentement», il est indiqué que «[l]orsqu'il envisage de choisir le consentement comme base juridique, le demandeur

[5] Par exemple, dans la section «Exigences relatives à la protection des données à caractère personnel dès la conception» (R10), page 49 des critères de certification, il est fait référence à l'article 25, paragraphe 1, du RGPD dans la note de bas de page 85.
[6] Par exemple, dans la section «Exigences relatives aux droits des personnes concernées (R15)», il n'est pas fait référence à l'article 12 du RGPD et ce dernier ne figure pas non plus à l'annexe 5 en ce qui concerne les «exigences relatives aux droits des personnes concernées».
[7] Voir p. 108, «un processus qui garantit que les données ne peuvent plus être utilisées pour identifier la personne à laquelle elles se rapportent, que des données distinctes relatives à la même personne ne peuvent pas être reliées entre elles et qu'aucune information sur une personne ne peut être déduite».
[8] L'EDPB souligne également que la définition peut nécessiter une adaptation à la suite d'orientations supplémentaires de sa part ou de la jurisprudence de la CJUE.

[...] veille également, lorsque la personne concernée est un mineur âgé de moins de 16 ans, à ce que le consentement soit donné ou autorisé par le titulaire de la responsabilité parentale». Le comité fait remarquer que, conformément à l'article 8, paragraphe 1, du RGPD, les législations nationales des États membres peuvent fixer des limites d'âge différentes. Toutefois, le comité n'a trouvé aucune référence dans les critères au droit national qui prévoit une limite d'âge inférieure lorsque l'article 6, paragraphe 1, point a), du RGPD s'applique, en ce qui concerne l'offre directe de services de la société de l'information aux enfants, conformément à l'article 8, paragraphe 1, du RGPD. Par conséquent, le comité recommande à l'AC FR d'exiger du propriétaire du système qu'il modifie ce critère en conséquence.

10. En outre, en ce qui concerne le projet de critère R06-S03-C02, le comité comprend également que l'organisme de certification procédera toujours à une évaluation des résultats documentés de la vérification effectuée, afin de s'assurer que les conditions spécifiques applicables au consentement sont remplies conformément à l'article 7 du RGPD. À cet égard, le comité recommande à l'AC FR d'exiger du propriétaire du système qu'il couvre également les exigences découlant de l'article 8, paragraphe 2, du RGPD.

2.3 PRINCIPES DE L'ARTICLE 5

11. Le comité accueille favorablement la section 5.3 du projet de critères, et en particulier le critère R05-S03-C01 relatif aux principes d'équité et de transparence, ainsi que les politiques pertinentes. Il fait observer que s'il existe des critères détaillés pour le principe de transparence, ce n'est pas le cas pour le principe d'équité. Dans ce contexte, le comité rappelle que les critères de certification doivent être un document autonome, dans lequel tous les critères sont suffisamment et spécifiquement élaborés pour pouvoir être audités. À cet égard, le comité note que, dans ses lignes directrices 04/2019 relatives à l'article 25 du RGPD «Protection des données dès la conception et la protection des données par défaut» (adoptées le 20 octobre 2020), il énumère plusieurs éléments qui devraient être pris en compte afin de respecter le principe d'équité. Par conséquent, par souci d'exhaustivité et de vérifiabilité des critères, le comité recommande à l'AC FR d'exiger du propriétaire du système qu'il continue d'élaborer des critères spécifiques, précis et vérifiables, dans la mesure où ils ne sont pas déjà couverts par d'autres parties des critères, sur la base de tous les éléments énumérés dans les lignes directrices 4/2019 de l'EDPB relatives à l'article 25 du RGPD concernant la protection des données dès la conception et la protection des données par défaut, point 70[9].

12. Au chapitre 5.4 S04 «Exigences relatives aux finalités», le système définit les exigences du principe de limitation de la finalité et le critère R05-S04-C01 interdit le traitement ultérieur de données à caractère personnel à des fins incompatibles avec les finalités spécifiées, explicites et légitimes pour lesquelles les données ont été initialement collectées. Toutefois, les dispositions de l'article 6, paragraphe 4, du RGPD relatives à la vérification de la compatibilité en vue d'un traitement ultérieur ne sont pas pleinement prises en compte dans les critères. Par conséquent, le comité recommande à l'autorité de contrôle compétente d'exiger du propriétaire du système qu'il continue d'élaborer

[9] Voir l'avis 18/2024 de l'EDPB sur le projet de décision de l'autorité de contrôle autrichienne concernant les critères de certification de DSGVO-zt GmbH, adopté le 16 juillet 2024, point 22.

des critères de certification spécifiques afin de couvrir pleinement les exigences de l'article 6, paragraphe 4, du RGPD.

2.3. OBLIGATIONS GÉNÉRALES DES RESPONSABLES DU TRAITEMENT

2.3.1. Obligations applicables aux responsables du traitement

13. En ce qui concerne la section 1.2 «Exigences relatives aux politiques en matière de protection des données à caractère personnel», le comité se félicite de la liste des informations à fournir aux personnes concernées. Toutefois, il note que le projet de critères de certification ne fait pas référence à l'article 13, paragraphe 3, du RGPD, qui dispose que «[l]orsqu'il a l'intention d'effectuer un traitement ultérieur des données à caractère personnel pour une finalité autre que celle pour laquelle les données à caractère personnel ont été collectées, le responsable du traitement fournit au préalable à la personne concernée des informations au sujet de cette autre finalité et toute autre information pertinente visée [au paragraphe 2]». Par souci d'exhaustivité des critères de cette section, le comité recommande à l'AC FR d'exiger du propriétaire du système qu'il révise les critères afin de couvrir les exigences de l'article 13, paragraphe 3, du RGPD.

14. Le comité fait remarquer que le projet de critères de certification exige que les demandeurs désignent un DPD. L'EDPB se félicite également du fait que le projet de critères de certification impose au DPD de rendre compte directement au niveau de l'encadrement le plus élevé, conformément au projet de critère R02-S04-C01, ce qui est conforme à l'article 38, paragraphe 3, du RGPD, et que le demandeur établit un réseau d'intermédiaires du DPD conformément au projet de critère R03-S01-C03. De l'avis du comité, les DPD peuvent effectivement mieux s'acquitter de leurs tâches s'ils interagissent avec des salariés à tous les niveaux hiérarchiques au sein de la structure du demandeur. Toutefois, l'EDPB encourage l'autorité de contrôle compétente à exiger du propriétaire du système qu'il inclue une définition du terme «intermédiaires», y compris des explications sur leur rôle vis-à-vis du DPD.

15. En outre, le projet de critère R02-S05-C01 exige que le demandeur fournisse chaque année au DPD un budget spécifique pour l'accomplissement de ses tâches. Toutefois, l'article 38, paragraphe 2, du RGPD dispose ce qui suit: «[l]e responsable du traitement et le sous-traitant aident le délégué à la protection des données à exercer les missions visées à l'article 39 en fournissant les ressources nécessaires pour exercer ces missions, ainsi que l'accès aux données à caractère personnel et aux opérations de traitement, et lui permettant d'entretenir ses connaissances spécialisées», ce qui signifie qu'il fait référence au terme plus général «ressources», qui inclut également le temps, la formation et l'équipement. Pour cette raison, l'EDPB recommande à l'AC FR d'exiger du propriétaire du système qu'il adapte les critères, de sorte que les ressources allouées au DPD couvrent non seulement l'exécution des tâches, mais aussi l'entretien des connaissances, conformément à l'article 38, paragraphe 2, du RGPD.

2.4 DROITS DES PERSONNES CONCERNÉES

16. Le comité observe que, dans le cadre du projet de critère R15-S02-C03 concernant le «délai de réponse»[10] aux demandes d'exercice des droits des personnes concernées, «le demandeur répond aux demandes d'exercice des droits dans un délai d'un mois à compter de la réception de la demande». Il relève que le projet de critère ne fait pas référence aux dispositions pertinentes de l'article 12 du RGPD et souligne qu'en vertu de l'article 12, paragraphe 3, du RGPD, un responsable du traitement fournit des informations sur les mesures prises à la suite d'une demande formulée en application des articles 15 à 22 «dans les meilleurs délais»[11]. Par conséquent, le comité recommande à l'AC FR d'exiger du propriétaire du système qu'il adapte les critères pertinents, afin de veiller à ce que les demandeurs fournissent des informations sur les mesures prises dans les meilleurs délais et au plus tard dans un délai d'un mois à compter de la réception de la demande.

17. Le comité note que l'article 13, paragraphe 2, point c), du RGPD exige que les informations à fournir aux personnes concernées comprennent le droit de retirer son consentement, le cas échéant. À cet égard, il fait remarquer que cette possibilité n'est pas mentionnée dans les projets de critères R01-S02-C04, R01-S02-C08 et R01-S02-C11. Par conséquent, le comité recommande à l'AC FR d'exiger du propriétaire du système qu'il modifie ces critères en conséquence afin que cette exigence soit également prise en compte dans les politiques des demandeurs.

2.5 RISQUES POUR LES DROITS ET LES LIBERTÉS DES PERSONNES PHYSIQUES ET MESURES TECHNIQUES ET ORGANISATIONNELLES QUI GARANTISSENT LA PROTECTION

18. Conformément à l'article 25, paragraphe 1, du RGPD, l'obligation de protection des données dès la conception s'applique «tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même». Toutefois, le comité note que le libellé du projet de critère R10-S02-C01 donne l'impression que seules les opérations de traitement mises en place au cours des deux dernières années sont soumises au respect de l'obligation de protection des données dès la conception. À cet égard, l'EDPB recommande à l'autorité de contrôle compétente d'exiger du propriétaire du système qu'il reformule le passage pertinent d'une manière qui précise que la certification exige l'évaluation de toutes les opérations de traitement relevant du champ d'application de la cible de l'évaluation en ce qui concerne l'obligation de protection des données dès la conception, quelle que soit la date à laquelle les opérations de traitement ont été engagées.

19. L'EDPB se félicite que le projet de critère R10-S02-C03 exige des demandeurs qu'ils effectuent un audit annuel conformément au projet de critère R01-S03-C04, afin de

[10] Fait partie du critère «15. Exigences relatives aux droits des personnes concernées (R15)».
[11] Voir également le considérant 59 du RGPD.

s'assurer que la procédure de protection des données dès la conception est appliquée. Toutefois, l'EDPB estime que cette exigence devrait être complétée par des procédures garantissant que des ajustements peuvent être apportés en permanence aux mesures individuelles adoptées par les demandeurs, afin de garantir la protection des données dès la conception conformément à l'article 25, paragraphe 1, du RGPD[12]. Par conséquent, l'EDPB recommande à l'AC FR d'exiger du propriétaire du système qu'il adapte les critères de la section 10.2 (par exemple dans le projet de critère R10-S02-C02) afin que les critères exigent des demandeurs qu'ils mettent en œuvre des procédures d'ajustement continu des mesures adoptées pour se conformer à l'article 25, paragraphe 1, du RGPD.

20. Dans les projets de critères R13-S03 et R13-S05, le système de certification fait référence aux mesures nécessaires que le demandeur devrait mettre en œuvre pour atténuer les risques recensés dans l'analyse d'impact relative à la protection des données (AIPD). Le comité relève que le système utilise le terme «mesures correctrices» à cet égard. Ce choix terminologique n'est pas clair, étant donné que le terme «correctrices» fait référence aux pouvoirs des APD, à l'article 58, paragraphe 2, du RGPD. Par conséquent, l'EDPB encourage l'autorité de contrôle compétente à exiger du propriétaire du système qu'il précise que le terme «mesures correctrices» ne fait pas référence aux pouvoirs des autorités chargées de la protection des données d'adopter des mesures correctrices, mais aux mesures d'atténuation en ce qui concerne la non-conformité.

2.6 MESURES TECHNIQUES ET ORGANISATIONNELLES QUI GARANTISSENT LA PROTECTION

21. Le comité observe que le projet de critère R14-S09-C02 «Procédure de développement de logiciels — contenu» fait référence au contenu de la procédure relative aux développements logiciels. Il note également que le projet de critère R14-S17-C02 comprend une procédure de sauvegarde. Par souci d'exhaustivité du critère R14-S09-C02, le comité estime qu'il est important d'y inclure également une procédure de sauvegarde. Par conséquent, il encourage l'autorité de contrôle compétente à exiger du propriétaire du système qu'il prévoie un processus de sauvegarde avant toute mise à niveau ou déploiement de logiciels.

22. En ce qui concerne le projet de critère R14-S19-C05 «Surveillance de l'activité du réseau», le comité se félicite de l'inclusion de la déclaration selon laquelle «le demandeur dispose d'un logiciel lui permettant d'analyser l'activité sur son réseau dans les conditions visées au critère R14-S18-C06». Toutefois, compte tenu du fait que le projet de critères exige que le demandeur établisse une procédure pour chaque activité de traitement, le comité recommande à l'autorité de contrôle compétente d'exiger du propriétaire du système qu'il modifie ce critère, et qu'il exige également du demandeur qu'il mette en place une procédure de suivi des activités du réseau permettant d'analyser l'activité sur son réseau dans les conditions visées dans le projet de critère R14-S18-C06.

[12] Lignes directrices 4/2019 de l'EDPB relatives à l'article 25 sur la protection des données dès la conception et la protection des données par défaut, adoptées le 13 novembre 2019 pour consultation publique et adoptées le 20 octobre 2020 après consultation publique, point 3.

3 CONCLUSIONS / RECOMMANDATIONS

En conclusion, l'EDPB considère ce qui suit:

23. En ce qui concerne les «observations générales», le comité formule les recommandations suivantes à l'AC FR:

1. exiger du propriétaire du système qu'il renforce la granularité de l'annexe 5 en fournissant des précisions supplémentaires sur la correspondance entre les dispositions du RGPD et les critères de certification, afin de déterminer facilement les critères permettant à un demandeur de démontrer qu'il respecte le RGPD. À titre subsidiaire, le comité recommande à l'AC FR d'exiger du propriétaire du système qu'il fasse référence à la disposition pertinente du RGPD pour chaque critère dans l'ensemble du document relatif aux critères de certification;

2. exiger du propriétaire du système, si une définition du terme «anonymisation» est nécessaire, qu'il veille à ce que ce terme soit défini conformément au considérant 26 du RGPD.

24. En ce qui concerne la «base juridique — consentement», le comité formule les recommandations suivantes à l'AC FR:

1. exiger du propriétaire du système qu'il renvoie, dans le critère R06-S03-C02, à la législation nationale qui prévoit une limite d'âge inférieure lorsque l'article 6, paragraphe 1, point a), du RGPD s'applique, en ce qui concerne l'offre directe de services de la société de l'information aux enfants, conformément à l'article 8, paragraphe 1, du RGPD;

2. exiger du propriétaire du système, en ce qui concerne le critère R06-S03-C02, qu'il couvre également les exigences découlant de l'article 8, paragraphe 2, du RGPD.

25. En ce qui concerne les «principes de l'article 5», le comité formule les recommandations suivantes à l'AC FR:

1. exiger du propriétaire du système qu'il développe des critères spécifiques afin de couvrir pleinement les dispositions de l'article 6, paragraphe 4, du RGPD relatives à la vérification de la compatibilité pour le traitement ultérieur;

2. exiger du propriétaire du système qu'il développe des critères spécifiques, précis et vérifiables, dans la mesure où ils ne sont pas déjà couverts par d'autres parties des critères, sur la base de tous les éléments énumérés dans les lignes directrices 4/2019 de l'EDPB relatives à l'article 25 du RGPD concernant la protection des données dès la conception et la protection des données par défaut, point 70.

26. En ce qui concerne les «obligations générales incombant aux responsables du traitement et aux sous-traitants», le comité formule les recommandations suivantes à l'AC FR:

1. exiger du propriétaire du système, par souci d'exhaustivité, qu'il ajoute à la section 1.2 des critères de certification la disposition de l'article 13, paragraphe 3, du RGPD, à savoir «[l]orsqu'il a l'intention d'effectuer un traitement ultérieur des données à caractère personnel pour une finalité autre que celle pour laquelle les données à caractère personnel ont été collectées, le responsable du traitement fournit au préalable à la personne concernée des

informations au sujet de cette autre finalité et toute autre information pertinente visée [au paragraphe 2]»;

2. exiger du propriétaire du système qu'il adapte le critère R02-S05-C01 afin de préciser que les ressources allouées au DPD couvrent non seulement l'exécution des tâches, mais également l'entretien des connaissances, conformément à l'article 38, paragraphe 2, du RGPD.

27. En ce qui concerne les «droits des personnes concernées», le comité formule les recommandations suivantes à l'AC FR:

1. exiger du propriétaire du système qu'il adapte le critère R15-S02-C03, afin de veiller à ce que les demandeurs fournissent des informations sur les mesures prises dans les meilleurs délais et au plus tard dans un délai d'un mois à compter de la réception de la demande;

2. exiger du propriétaire du système qu'il révise les critères R01-S02-C04, R01-S02-C08 et R01-S02-C11 afin d'inclure les obligations de l'article 13, paragraphe 2, point c), du RGPD, qui prévoit que les informations à fournir aux personnes concernées comprennent le droit de retirer son consentement, le cas échéant.

28. En ce qui concerne les «risques pour les droits et libertés des personnes physiques» et les «mesures techniques et organisationnelles garantissant la protection», le comité formule les recommandations suivantes à l'AC FR:

1. exiger du propriétaire du système qu'il reformule le passage pertinent du critère R10 S02-C01 d'une manière qui précise que cette certification exige l'évaluation de toutes les opérations de traitement relevant du champ d'application de la cible de l'évaluation en ce qui concerne l'obligation de protection des données dès la conception, indépendamment du moment où les opérations de traitement ont été engagées;

2. exiger du propriétaire du système qu'il adapte les critères de la section 10.2 (par exemple dans le projet de critère R10-S02-C02) visant à ce que les critères imposent aux demandeurs de mettre en œuvre des procédures d'ajustement continu des mesures adoptées pour se conformer à l'article 25, paragraphe 1, du RGPD;

3. exiger du propriétaire du système qu'il modifie le critère R14-S19-C05 et qu'il exige également que le demandeur mette en place une procédure de surveillance de l'activité du réseau permettant d'analyser l'activité sur son réseau dans les conditions visées dans le projet de critère R14-S18-C06.

29. Enfin, conformément aux lignes directrices, l'EDPB rappelle également que, en cas de changement des critères de certification impliquant des modifications substantielles[13], l'AC FR devra en soumettre la version modifiée à l'EDPB conformément à l'article 42, paragraphe 5, et à l'article 43, paragraphe 2, point b), du RGPD.

[13] Voir la section 9 de l'addendum aux lignes directrices 1/2018 sur la certification et la définition des critères de certification conformément aux articles 42 et 43 du règlement fournissant des «orientations sur l'évaluation des critères de certification» pour lesquelles la période de consultation publique a expiré le 26 mai 2021.

4 OBSERVATIONS FINALES

30. Le présent avis est adressé à l'AC FR et sera publié conformément à l'article 64, paragraphe 5, point b), du RGPD.

31. Conformément à l'article 64, paragraphes 7 et 8, du RGPD, l'AC FR communique au président sa réponse au présent avis par voie électronique, dans un délai de deux semaines suivant la réception de l'avis et indique si elle maintiendra ou si elle modifiera son projet de décision. Dans le même délai, elle fournit le projet de décision modifié ou, si elle n'a pas l'intention de suivre l'avis du comité, en tout ou en partie, elle fournit les motifs pertinents pour lesquels elle n'a pas l'intention de suivre cet avis.

32. Conformément à l'article 70, paragraphe 1, point y), du RGPD, l'AC FR communique la décision finale à l'EDPB pour inclusion dans le registre des décisions soumises au mécanisme de contrôle de la cohérence.

33. L'EDPB rappelle que, conformément à l'article 43, paragraphe 6, du RGPD, l'AC FR rend publics les critères de la certification Lexing sous une forme aisément accessible et les transmet au comité en vue de leur inscription dans le registre public des mécanismes de certification et des labels de protection des données, conformément à l'article 42, paragraphe 8, du RGPD.

Pour le comité européen de la protection des données
La présidente

(Anu Talus)