

Documents de l'EDPB



Document du CEPD relatif à la procédure d'approbation des critères de certification par le CEPD aboutissant à une certification commune, le label européen de protection des données

Adopté le 28 janvier 2020

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

Table des matières

1. APPROBATION par le CEPD de critères de certification à l'échelle de l'UE (label UE de protection des données): EXAMEN, SOUMISSION, RECEVABILITÉ et ADOPTION	3
1.1. Soumission	3
1.2. Recevabilité initiale des critères de certification	4
1.3. Coopération (phase de coopération informelle au niveau des autorités de contrôle)	4
1.4. Soumission et approbation formelle (phase devant le CEPD)	5
1.5. Avis visé à l'article 64, paragraphe 2.....	6
1.6. Étapes suivant l'avis du CEPD	7
Déroulement de la procédure — Approbation par le CEPD du label de l'UE relatif à la protection des données — Critères de certification.....	8

Le comité européen de la protection des données,

vu l'article 42, paragraphe 5, l'article 64, paragraphe 2, et l'article 70, paragraphe 1, point o), 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, et en particulier son annexe XI et son protocole 37, tels que modifiés par la décision du Comité mixte de l'EEE n° 154/2018 du 6 juillet 2018¹,

vu les articles 3 et 22 de son règlement intérieur du 25 mai 2018,

A ADOPTÉ LE DOCUMENT SUIVANT:

1. APPROBATION par le CEPD de critères de certification à l'échelle de l'UE (label UE de protection des données): EXAMEN, SOUMISSION, RECEVABILITÉ et ADOPTION

1.1. Soumission

Les propriétaires de systèmes de certification (il peut s'agir d'organisations ou de sociétés privées qui ne sont pas chargées de délivrer des certificats) ou les organismes de certification doivent soumettre formellement leurs critères de certification à l'échelle de l'UE (dans l'ordre d'application):

- 1) auprès de l'autorité de contrôle compétente (ACC) du lieu où les propriétaires de système² ont leur siège;
- 2) auprès de l'ACC du lieu où l'organisme de certification appliquant le mécanisme de certification a son siège³, en tenant compte de l'État membre dans lequel la plupart des certificats seront probablement délivrés.

Par ailleurs, les autorités de contrôle (AC) peuvent également prendre l'initiative d'élaborer elles-mêmes des critères de certification pour un mécanisme de certification à l'échelle de l'UE⁴.

Conformément à l'article 63 et à l'article 70, paragraphe 1, point o), les autorités de contrôle peuvent soumettre des critères au sens de l'article 42, paragraphe 5, pour un mécanisme de certification à l'échelle de l'UE, à l'approbation du CEPD⁵. Les autorités de contrôle procéderont à un examen afin de

¹ Les références à l'«UE» figurant dans le présent document doivent s'entendre comme des références à l'«EEE».

² Un propriétaire de système peut également être un organisme de certification

³ La délivrance de l'agrément à l'organisme de certification (soit par l'organisme national d'accréditation, soit par l'ACC) comprend également une évaluation du mécanisme de certification. Elle inclut notamment une vérification du caractère approprié des méthodes d'évaluation proposées au regard des critères de certification approuvés. L'agrément sera également délivré à l'endroit où l'organisme de certification a son siège, conformément au point 44 des lignes directrices 1/2018 du CEPD.

⁴ L'AC agira en qualité de propriétaire du système.

⁵ Une AC ne peut pas demander un avis sur des critères de certification si elle n'a pas soumis au préalable ses exigences en matière d'agrément pour approbation.

s'assurer que les projets de critères de certification sont conformes aux exigences du RGDP en matière de critères de certification à l'échelle de l'UE, en tenant compte des lignes directrices du CEPD en matière de certification⁶. Afin de faciliter l'examen de l'ACC, le modèle d'évaluation des critères de certification adopté par le CEPD devra être rempli intégralement (il faut remplir tant la partie nationale que la partie sur l'UE). Il n'est possible de soumettre ce document au CEPD que si l'ACC estime que les critères sont susceptibles d'être approuvés par le CEPD (voir étape 3a)⁷.

1.2. Recevabilité initiale des critères de certification

Si l'ACC juge le projet de critères irrecevable, elle écrit au propriétaire de système en exposant les motifs de sa décision (voir étape 3b).

Si l'ACC juge le projet de critères recevable, elle en informe le propriétaire de système par écrit, en confirmant l'ouverture de l'étape suivante de la procédure et l'évaluation du projet de critères, ce qui déclenche la procédure de coopération informelle décrite ci-dessous, visant à évaluer les critères en vue de leur approbation.

1.3. Coopération (phase de coopération informelle au niveau des autorités de contrôle)

La phase de coopération informelle est primordiale pour l'efficacité de la procédure d'approbation du comité. Cette phase permettra à l'ACC désignée ci-dessus de diriger l'évaluation des critères et de fournir un retour d'information au propriétaire de système le cas échéant. L'ACC avisera le propriétaire de système en temps utile, à chaque phase de la procédure.

L'ACC émettra une notification communiquant sa position à toutes les autorités de contrôle et lancera un appel à volontaires, pour trouver deux co-examineurs au maximum pour l'aider à évaluer le contenu des critères (voir étape 4). L'appel concernant les co-examineurs est adressé par courriel au secrétariat du CEPD. Le courriel doit contenir le modèle d'évaluation du CEPD rempli par l'ACC.

La phase de coopération informelle (voir étapes 4 à 6) ne peut commencer que lorsque les documents suivants sont disponibles en anglais et peuvent être communiqués à d'autres autorités de contrôle:

- le modèle d'évaluation du CEPD entièrement rempli par l'ACC. Il comprendra des informations sur la manière dont toutes les législations nationales pertinentes ont été prises en compte et sur le déploiement prévu dans les États membres; et
- une copie des critères de certification et de toute annexe pertinente.

Les critères de certification liés à une législation nationale spécifique peuvent être soumis dans la langue de cet État membre, s'ils sont disponibles.

Le rôle des co-examineurs sera d'aider l'ACC à évaluer le projet de critères. Les co-examineurs doivent veiller à associer des experts, en fonction de la matière sujette à certification. Une fois les co-examineurs confirmés, ils doivent présenter leurs observations sur les critères dans les trente jours suivant la date où les documents leur ont été transmis. Ces observations seront ensuite prises en compte par l'ACC lors de son évaluation. L'examen portera principalement sur la recevabilité technique des critères de certification (voir étape 5).

⁶ Lignes directrices 1/2018 relatives à la certification et à la définition des critères de certification conformément aux articles 42 et 43 du règlement

⁷ Voir la section 4.2 (points 35 à 45) des lignes directrices du CEPD sur les critères de certification.

À la suite du co-examen, l'ACC transmettra le projet de critères à toutes les autorités de contrôle. Le secrétariat du CEPD peut apporter son assistance dans la communication entre les autorités de contrôle (voir étape 6). Toutes les autorités de contrôle concernées disposent d'un délai de réponse de 30 jours et toute question importante peut être soumise au sous-groupe du CEPD pertinent pour y être discutée. L'examen consistera à s'assurer que la législation nationale a été correctement prise en compte et inclura également l'analyse de la conformité des critères relatifs à la législation nationale. Si les autorités de contrôle ne répondent pas, les critères passent à l'étape suivante de la procédure.

L'ACC peut décider de répéter les étapes 5 et 6 si nécessaire.

L'ACC peut, à tout stade de la phase de coopération informelle, donner au propriétaire de système la possibilité de modifier les critères de certification en tenant compte des remarques des autorités de contrôle.

Après l'étape 6 et dans l'hypothèse d'un résultat positif, l'ACC demandera une réunion de sous-groupe pour débattre des critères examinés (voir étape 7). L'ACC actualisera le modèle d'évaluation du CEPD avec les principales conclusions de cette réunion. Toute action évoquée durant la réunion peut être menée à bien par l'ACC et les critères peuvent être révisés par le propriétaire de système.

À l'issue de la phase de coopération informelle, l'ACC (en consultation avec le propriétaire de système) peut décider de soumettre ou non les critères de certification au CEPD en vue d'une approbation formelle. C'est l'ACC qui décide en dernier lieu si le projet de critères doit être soumis au comité pour approbation comme prévu à l'article 63 du RGPD. Lorsque l'ACC décide de ne pas soumettre les critères de certification au CEPD, la procédure prend fin (voir étape 8b). Une nouvelle présentation des critères de certification, à une date ultérieure, donnera lieu à un nouvel examen.

Le propriétaire de système doit participer à la procédure d'examen au cours de la phase informelle. L'ACC doit informer le propriétaire de système des observations formulées durant la phase de coopération et ce dernier doit avoir la possibilité de demander des éclaircissements et de présenter ses propres observations⁸.

1.4. Soumission et approbation formelle (phase devant le CEPD)

L'approbation d'un label UE de protection des données a lieu dans le cadre de la procédure d'avis visée à l'article 64, paragraphe 2.

L'ACC est priée de tenir compte du calendrier de travail du sous-groupe d'experts (ESG) «Conformité, e-Gouvernement et Santé» (CEH) avant de procéder à sa soumission par IMI.

La soumission formelle doit être effectuée par l'intermédiaire de la plateforme IMI (étape 8a). Elle doit remplir les critères de recevabilité suivants pour être acceptée par le CEPD:

- tous les documents pertinents doivent être présentés en anglais;
- le modèle d'évaluation du CEPD doit être rempli par l'ACC et soumis (le modèle doit être modifié en fonction du résultat de la phase d'examen initiale); et
- une copie des critères de certification et des éventuelles annexes doit être fournie.

⁸ L'ACC doit s'assurer que le propriétaire de système est informé de cette possibilité et qu'il peut en bénéficier.

Le secrétariat vérifiera que tous les documents sont présents et complets. Le secrétariat peut demander à l'ACC de fournir, dans un certain délai, toute information supplémentaire nécessaire pour compléter le dossier. En règle générale, et sans préjudice des autres traductions éventuellement nécessaires ou exigées par la loi, tous les documents pertinents doivent être fournis par le demandeur dans la langue de l'ACC et également en anglais. Le cas échéant, par exemple en présence de documents qui ne proviennent pas de l'autorité de contrôle ou qui ne sont pas rédigés par cette dernière, les documents soumis par l'ACC seront traduits en anglais par le secrétariat dans les meilleurs délais. En pareil cas, lorsque l'autorité compétente accepte la traduction et que le président et l'ACC décident que le dossier est complet, le secrétariat transmet, au nom du président, le dossier aux membres du comité.

L'avis du comité est adopté dans un délai de huit semaines après que le président et l'ACC (selon le cas) ont décidé que le dossier était complet. Ce délai peut être prolongé de six semaines en fonction de la complexité de la question, sur décision du président, de sa propre initiative ou à la demande d'au moins un tiers des membres du comité.

Le secrétariat, en collaboration avec un rapporteur et des membres des sous-groupes d'experts si le président en décide ainsi, prépare et rédige les projets d'avis avant de les soumettre au vote du comité. En fonction de la portée du mécanisme de certification, il peut être nécessaire de faire appel à l'expertise d'autres sous-groupes du CEPD afin de préparer les avis.

Sur décision du président, une équipe de rédaction peut être mise en place, en fonction de la date de la soumission, par courriel ou à l'occasion d'une réunion CEH. L'appel à volontaires pour l'équipe de rédaction sera effectué par le secrétariat, en collaboration avec les coordinateurs des groupes d'experts CEH. Afin d'éviter les conflits d'intérêts, l'ACC ne doit pas faire partie de l'équipe de rédaction principale. Toutefois, l'équipe de rédaction principale peut toujours adresser des questions à l'ACC.

Le secrétariat et l'équipe de rédaction (le cas échéant) examinent les critères de certification soumis et les documents justificatifs (y compris le modèle d'évaluation) puis rédigent un projet d'avis. Ce faisant, ils devront toujours tenir compte de ce qui a été indiqué dans des avis antérieurs traitant du même sujet, afin de garantir la cohérence. Le modèle d'évaluation du CEPD soumis par l'ACC peut être utilisé comme document de travail interne lors de l'élaboration du projet d'avis. Cet examen doit être réalisé dans les délais relatifs à l'avis.

1.5. Avis visé à l'article 64, paragraphe 2

Au titre de l'article 64, paragraphe 2 et de l'article 70, paragraphe 1, point b), le CEPD émet un avis et donne son approbation sur les sujets décrits à l'article 42, paragraphe 5, du RGPD (étape 9)⁹.

Les règles de l'article 10 du règlement intérieur du CEPD régissent l'adoption d'un avis¹⁰. L'autorité de contrôle qui décide de demander un avis au titre de l'article 64, paragraphe 2, devra fournir une motivation écrite de sa demande, conformément à l'article 10, paragraphe 3, du règlement intérieur.

⁹L'article 64, paragraphe 2, du RGPD autorise les autorités de contrôle à demander un avis concernant une question d'application générale ou produisant des effets dans plusieurs États membres. Étant donné que le label UE de protection des données a des effets à l'échelle de l'UE, l'avis du comité relève du champ d'application de l'article 64, paragraphe 2, plutôt que de l'article 64, paragraphe 1.

¹⁰Il convient également de noter que les seules options possibles sont l'approbation ou le rejet car «approuver» un label avec des questions non encore résolues serait source de confusion.

Dans le contexte d'une demande d'approbation, par le CEPD, d'un label européen de protection des données pour des critères de certification, l'ACC doit demander un avis au titre de l'article 64, paragraphe 2, sur une question produisant des effets dans plusieurs États membres.

Le processus d'approbation du CEPD prend fin avec l'approbation ou le rejet de la demande relative à un label UE de protection des données concernant les critères soumis. Aucun suivi de l'avis du comité n'est nécessaire conformément à l'article 64, paragraphe 2.

L'avis rendu par le CEPD au titre de l'article 64, paragraphe 2, est applicable dans tous les États membres¹¹.

1.6. Étapes suivant l'avis du CEPD

Les étapes succédant à l'adoption, par le CEPD, de l'avis relatif au label UE de protection des données sont les suivantes:

- le secrétariat publie l'avis contenant l'approbation ou le rejet du label de protection des données par le CEPD;

Si le CEPD rejette la demande de label UE de protection des données en rendant un avis négatif:

- l'ACC informe le propriétaire de système de l'issue de la procédure d'approbation du CEPD relative à la demande de label UE de protection des données;
- l'ACC chef de file/coordinatrice se charge de la transmission des documents requis au secrétariat, en vue de leur publication au registre public du CEPD.

Si le CEPD rejette la demande de label UE de protection des données en rendant un avis négatif:

- l'ACC informe le propriétaire de système que, selon l'avis du CEPD, le mécanisme de certification ne répond pas aux exigences requises pour être approuvé par le CEPD;
- l'ACC peut décider de soumettre à nouveau des critères de certification pour demander un label UE de protection des données. L'ACC peut décider soit d'entamer une nouvelle phase de coopération informelle, soit d'appliquer directement aux critères la phase d'avis visée à l'article 64, paragraphe 2.

Des orientations relatives aux compétences de la Commission européenne au titre de l'article 43, paragraphes 8 et 9, seront ajoutées en temps utile, ainsi que toute autre exigence relative aux critères en matière de transfert international.

¹¹Si une autorité de contrôle ne suit pas l'avis émis et n'accepte pas l'approbation du label UE de protection des données, la question peut être portée devant le comité par une autre autorité de contrôle ou par la Commission afin d'obtenir une décision contraignante en vertu de l'article 65, paragraphe 1, point c)¹¹.

Déroulement de la procédure — Approbation par le CEPD du label de l'UE relatif à la protection des données — Critères de certification

