Exigences spécifiques d'accréditation des organismes procédant à la certification des opérations de traitement de données personnelles

CERT CPS REF 54 - Révision 00

SOMMAIRE

1. OBJET 3
2. REFERENCES ET DEFINITIONS 3
2.1. Références 3
2.2. Abréviations et définitions 4
3. DOMAINE D'APPLICATION 4
4. MODALITES D'APPLICATION 4
5. MODIFICATIONS APPORTEES A L'EDITION PRECEDENTE 4
6. EXIGENCES A SATISFAIRE PAR L'ORGANISME DE CERTIFICATION 4
7. PROCESSUS D'ACCREDITATION 6
7.1. Généralités 6
7.2. Portée d'accréditation demandée 6
7.3. Modalités d'évaluation 6
7.4. Attestation d'accréditation 7
7.5. Confidentialité – Echange d'informations 7
7.6. Dispositions à prendre en cas de suspension, de retrait d'accréditation ou de cessation d'activité de l'organisme certificateur 8
7.7. Modalités de transition 8
8. MODALITES FINANCIERES 8

1. OBJET

Ce document définit les exigences à satisfaire et le processus d'accréditation pour la certification des opérations de traitement de données personnelles en vue d'établir la conformité au RGPD.

2. REFERENCES ET DEFINITIONS

2.1. Références

Ce document s'applique en complément des documents suivants :

- Pour toute demande d'accréditation pour une certification citée en objet :
  - Référentiel relatif aux exigences d'agrément des organismes de certification pour les mécanismes de certification approuvés au titre de l'article 42 du règlement général sur la protection des données, indiqué Référentiel CNIL 2022-095 dans le reste du document.
    (disponible sur https://www.cnil.fr/sites/cnil/files/atoms/files/referentiel_agrement-organismes-certification_mecanismes-certification.pdf ou https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000046374815)
  - EDPB Guidelines 4/2018 on the accreditation of Certification bodies under Article 43 GDPR

- Pour une demande concernant la certification EUROPRIVACY
  - Europrivacy Guidelines for Accreditation Procedure (EP-G.AC), version en vigueur
  - Europrivacy Certification Scheme (EP-CS.1), version en vigueur
  - Europrivacy List of Criteria, Checks and Controls (EP-C.ALL), incluant :
    - Les critères approuvés par l'EDPB :
      - Application and Target of Evaluation Preliminary Checks and Controls (EP-C.A)
      - Europrivacy GDPR Core Criteria (EP-C.G)
      - Technical and Organizational Measures Checks and Controls (EP-C.T)
      - Complementary Contextual Checks and Controls (EP-C.C)
    - Documentation Checklist for Europrivacy Certification (EP-C.D)
    - Complementary Surveillance Audit Checks and Controls (EP-C.S)
  - Europrivacy Scope Limitation
  - Europrivacy General Terms and Conditions (EP-P.TC)
  - Europrivacy Rules on the Use of Logo, Certificates and Marks of Conformity

Ces documents sont disponibles sur le site internet suivant :

https://www.europrivacy.com/index.php/en/ep/europrivacy-criteria

2.1.1. Publication de l'ISO

- NF EN ISO/IEC 17065 « Exigences pour les organismes certifiant les produits, les procédés et les services »
- NF EN ISO/IEC 17025 « Exigences générales concernant la compétence des laboratoires d'étalonnage et d'essais », (applicable aux ressources externes, cf. §6 du présent document)
- NF EN ISO/IEC 17021-1 « Evaluation de la conformité – Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management – Partie 1 : Exigences », (applicable au processus de certification, cf. § 6 du présent document)

2.1.2. Autres textes de référence

- 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 (règlement général sur la protection des données).

2.2. Abréviations et définitions

Les abréviations suivantes sont utilisées :

- OC : Organisme de Certification
- RGPD : Règlement Général sur la Protection des Données
- CNIL : Commission Nationale de l'Informatique et des Libertés
- EDPB : European Data Protection Board
- EP : Europrivacy
- ECCP : European Centre for Certification and Privacy

3. DOMAINE D'APPLICATION

Ce document s'applique à toutes les demandes d'accréditation et aux organismes accrédités pour la certification des opérations de traitement de données personnelles en application de l'article 43 du RGPD.
A ce jour, le présent document s'applique uniquement à la certification EUROPRIVACY.

4. MODALITES D'APPLICATION

Ce document est applicable à compter du 20/09/2024.

5. MODIFICATIONS APPORTEES A L'EDITION PRECEDENTE

Il s'agit de l'édition initiale du document.

6. EXIGENCES A SATISFAIRE PAR L'ORGANISME DE CERTIFICATION

Il appartient à tout organisme candidat ou accrédité d'appliquer les documents de référence cités au §2 et de prendre en compte la réglementation applicable en vigueur.
Dans la suite du document, seules les exigences spécifiques à EUROPRIVACY (EP) ont été indiquées, étant entendu que les exigences générales citées au § 2 s'appliquent.

	NF EN ISO/CEI 17065 : 2012 et Référentiel CNIL 2022-095	**EP-CS.1 version 4**	**Autres documents applicables et commentaires éventuels**
Programme de certification	3.9	2- 6	EP list of criteria, checks and controls Les critères d'évaluation doivent être affinés par l'OC et communiqués à ses clients pour chaque pays d'intervention. Les modalités d'évaluation correspondantes doivent être définies par l'OC et choisies parmi le catalogue proposé par EP. Ces modalités complètent le

			programme de certification EP et doivent être conformes au CERT REF 09.
Portée de la certification	3.10	2	EP certification scope limitations
Contrat de certification	4.1.2	7.2.2, 12.3	
Utilisation de marque de conformité	4.1.3	15.6	EP rules and guidelines on the use of certificates, logos and marks of conformity
Gestion de l'impartialité	4.2	13.1, 13.3 à 13.5	En plus des exigences de l'ISO/IEC 17065, les clauses §3.3, 5.2.5, 4.2.1 et 5.2.13 de l'ISO/IEC 17021-1 : 2015 s'appliquent.
Non-discrimination	4.4	5.2.9	
Confidentialité	4.5	15	
Informations accessibles au public	4.6	15.4	
Organisation et direction	5.1	12.1, 12.2	
Dispositif préservant l'impartialité	5.2	13.2	
Ressources externes	6.2.2.	8.3, 14.4.4	Quand les activités de tests sont sous-traitées, elles doivent être couvertes par une accréditation selon ISO/IEC 17025 :2015 (§ 8.3)
Personnel de l'OC - Ressources internes	6.1- 6.2.1	7.4, 14	EP Management of competencies of personnel involved in EP certifications
Revue de la demande	7.3	7.2 et 7.3	
Changement d'OC	7.3.5	9.4	
Evaluation	7.4	7.6, 7.7, 8	En sus, §9.5.3.1 de l'ISO/IEC 17021-1 :2015 s'applique
Résultats de l'évaluation	7.4.9	8.6.2 – 8.7	
Revue	7.5	9.1	
Décision de certification	7.6	9.2, 9.6	
Document de certification	7.7	9.6, 15.6	
Annuaire des produits certifiés	7.8	9.7, 15.4	
Surveillance	7.9	10	
Changement ayant des conséquences sur la certification	7.10	11, 15.3	
Résiliation, réduction, suspension ou retrait de certification	7.11	9.5	
Enregistrements	7.12	15.5	
Appels et plaintes	7.13	17	
Exigences du système de management	8	16	

Ce tableau est une aide à la compréhension de l'interaction des différentes exigences applicables aux OC mais ne constitue pas une liste exhaustive et reste à valeur indicative.

7. PROCESSUS D'ACCREDITATION

7.1. Généralités

7.1. Programme de certification

Le programme de certification doit :

- avoir été approuvé par la CNIL pour ce qui concerne les critères de certification et être conforme au document CERT REF 09 ou
- avoir été approuvé par l'EDPB pour ce qui concerne les critères de certification et analysé comme étant adéquat pour les besoins de l'accréditation selon les procédures de l'EA, dans le cas d'un programme européen ou international
- inclure les modalités d'évaluation que l'OC a choisi de mettre en œuvre pour la certification EUROPRIVACY.

7.1.2 Equipe d'évaluation

L'équipe d'évaluation chargée des opérations d'évaluation pour EUROPRIVACY comprend un ou plusieurs évaluateur(s) technique(s) compétent(s) dans le domaine du RGPD et satisfaisant aux exigences du schéma pour les évaluateurs.

7.2. Portée d'accréditation demandée

La portée de demande d'accréditation est établie selon les documents de nomenclature CERT CPS INF 02. La portée d'accréditation est considérée comme éligible à la portée flexible de type FLEX1, en application du document CERT REF 08.

7.3. Modalités d'évaluation

7.3.1 Modalités de candidature

Toute demande d'accréditation pour la délivrance de la certification EUROPRIVACY est traitée comme une demande d'accréditation initiale (si l'organisme n'est pas accrédité selon l'ISO/IEC 17065) ou d'extension majeure de la portée d'accréditation à un nouveau domaine selon la procédure prévue par le document CERT REF 05.

Toute extension relative à l'ajout d'un nouveau programme de certification s'appliquant à l'article 43 du RGPD, est considérée comme une extension majeure. Elle est traitée conformément au règlement d'accréditation CERT REF 05.

L'OC candidat devra fournir avec son dossier de candidature les modalités d'évaluation qu'il a choisi de mettre en œuvre parmi le catalogue proposé par EUROPRIVACY ainsi que l'autorisation délivrée par EUROPRIVACY telle que demandé dans le formulaire de candidature (document CERT FORM 29).
Ces modalités feront l'objet d'une analyse de référentiel en se basant sur le document CERT REF 09, afin de confirmer l'adéquation de ces modalités par rapport au dispositif Europrivacy.

Toute demande fera l'objet d'un examen documentaire de recevabilité approfondie conformément au règlement d'accréditation CERT REF 05.

Tel que précisé au § 3 du Référentiel CNIL 2022-095, la délivrance des certificats en vertu de l'article 43 du RGPD requiert d'avoir obtenu une décision favorable du COFRAC à la recevabilité opérationnelle suite à la revue de sa demande d'accréditation. L'OC dispose ensuite d'une période de 12 mois à compter de la date de la réponse favorable du COFRAC pour obtenir l'accréditation. A des fins d'évaluation d'accréditation, l'OC doit avoir réalisé des activités avant le jour de l'évaluation, à l'exception de la délivrance des certificats pour le dispositif Europrivacy, pour lequel les certificats ne pourront être émis qu'une fois l'accréditation prononcée.

7.3.2 Observations d'activités de certification

Une observation d'activité minimum doit être effectuée avant d'octroyer l'accréditation correspondante pour chaque programme de certification.

Le nombre d'observations sur un cycle d'accréditation est calculé conformément au document Europrivacy Guidelines for Accreditation Procedure :

- De 1 à 50 clients actifs : 1 observation
- De 51 à 100 clients actifs : 2 observations
- Plus de 100 clients actifs : 3 observations

Le programme des observations d'activité peut être adapté sur le cycle d'accréditation en fonction d'une analyse de risques spécifique réalisée par le COFRAC.

L'observation doit avoir une durée adéquate afin de couvrir l'analyse des éléments les plus importants du processus d'audit mené par l'OC et sera donc ajustée en fonction des activités observées.

Dans la mesure du possible, chaque observation concerne un type de traitements de données différent, objet de la portée d'accréditation et un auditeur différent. L'activité observée peut être un audit, des tests, la réunion d'un comité de certification, ou l'activité d'un sous-traitant entrant dans le champ de la portée d'accréditation considérée. Cette observation ne peut pas porter sur un audit à blanc.

Les observations doivent être réalisées sur une période allant d'un mois avant l'évaluation du siège de l'OC à 12 mois après.

7.4. Attestation d'accréditation

L'attestation d'accréditation délivrée est établie selon le document de nomenclature CERT CPS INF 02.

7.5. Confidentialité – Echange d'informations

Le Cofrac informe, dans les plus brefs délais, de la mesure d'octroi, d'extension, de suspension, de résiliation ou de retrait (total ou partiel) d'accréditation et de son motif, le propriétaire du programme de certification, ECCP ainsi que la CNIL.
Si le Cofrac reçoit de la part de la CNIL des informations concernant les OC accrédités pour ce domaine, elle sera tenue informée de leur analyse et des suites données. Toute information transmise est considérée comme une donnée d'entrée du suivi de l'accréditation.

7.6. Dispositions à prendre en cas de suspension, de retrait d'accréditation ou de cessation d'activité de l'organisme certificateur

Les dispositions de la procédure GEN PROC 03 s'appliquent. L'OC doit se référer aux § 7.9 et 7.11 du Référentiel CNIL n°2022-095 et contacter le propriétaire du programme de certification (ECCP) afin de connaitre les conséquences pour les certificats qu'il a délivrés et pour la continuité de ses activités de certification.

7.7. Modalités de transition

Seules les versions majeures (cf. §2.1.2) font l'objet d'un plan de transition, les versions mineures n'ayant pas d'impact sur l'accréditation délivrée. Pour autant, il appartient à l'OC accrédité de démontrer lors de chaque évaluation qu'il se tient à jour de toutes les évolutions de tous les documents, en informe ses clients, en mesure les conséquences, et met en œuvre les nouvelles dispositions, conformément au § 7.10 de l'ISO/IEC 17065 : 2012.

Lors de la publication d'une nouvelle version majeure, le Cofrac établit des modalités de transition.

L'OC accrédité ne peut revendiquer sa conformité au programme de certification modifié qu'après notification écrite du Cofrac.

8. MODALITES FINANCIERES

Les modalités énoncées dans les documents CERT REF 06 et CERT REF 07 s'appliquent, en considérant les activités de certification objet du présent document comme un domaine d'accréditation.