Délibération n° 2020-050 du 30 avril 2020 portant adoption d'un référentiel relatif à l'agrément des organismes chargés de contrôler le respect des codes de conduite

La Commission nationale de l'informatique et des libertés,

Vu la convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu le 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, notamment ses articles 41 et 57.1.p) ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu le décret n° 2019-536 du 29 mai 2019 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu les lignes directrices sur les codes de conduites et les organismes de contrôle de ces codes au sens du règlement (UE) 2016/679 adoptées le 4 juin 2019 par le Comité européen de la protection des données ;

Après avoir entendu Mme Anne DEBET, commissaire, en son rapport, et Mme Nacima BELKACEM, commissaire du Gouvernement, en ses observations,

Fait les observations suivantes :

1. L'article 41 du règlement général relatif à la protection des données (RGPD) prévoit que le contrôle du respect d'un code de conduite peut être effectué par un organisme qui dispose du niveau d'expertise approprié au regard de l'objet du code. Ces organismes doivent être agréés à cette fin par l'autorité de contrôle compétente.

2. L'article 57.1.p) du RGPD prévoit que chaque autorité de contrôle rédige et publie les exigences relatives à l'agrément des organismes chargés du suivi des codes de conduite en application de l'article 41.

3. L'article 41.3 du RGPD indique que les projets d'agrément établis par chaque autorité de contrôle au niveau national sont soumis au mécanisme de « contrôle de la cohérence » et doivent être communiqués au Comité européen de la protection des données (CEPD).

4. Le 3 octobre 2019, un projet d'agrément a été adopté par la Commission et soumis au CEPD le 18 octobre 2019. Le CEPD a adopté un avis favorable relatif à ce projet le 28 janvier 2020, qui a été notifié à la Commission le 4 février 2020.

Les données personnelles nécessaires à l'accomplissement des missions de la CNIL sont traitées dans des fichiers destinés à son usage exclusif. Les personnes concernées peuvent exercer leurs droits Informatique et Libertés en s'adressant au délégué à la protection des données (DPO) de la CNIL via un formulaire en ligne ou par courrier postal. Pour en savoir plus : www.cnil.fr/donnees-personnelles.

5. La présente délibération fixe les critères d'agrément des organismes chargés du contrôle du respect des codes de conduite, tels que visés à l'article 41 du règlement (UE) 2016/679.

Décide :

De l'adoption du référentiel d'agrément des organismes chargés du contrôle des codes de conduite, tel qu'annexé à la présente délibération.

La durée de l'agrément sera initialement fixée à cinq ans, sans préjudice de l'exercice à tout moment des compétences de la CNIL au regard des obligations de l'organisme de contrôle.

La procédure de demande initiale et de renouvellement d'un agrément est encadrée par le règlement intérieur de la CNIL. Le renouvellement entraîne un réexamen de l'éligibilité de l'organisme de contrôle, qui peut donner lieu à une décision favorable ou à un refus.

Cette décision sera publiée au Journal officiel de la République française.

La Présidente

M-L. D

Marie-Laure Denis

Annexe : référentiel d'agrément des organismes chargés de contrôler le respect des codes de conduite

Remarques générales :

L'article 40.4 du RGPD prévoit que les codes de conduites comprennent les mécanismes permettant à l'organisme visé à l'article 41 du règlement de contrôler le respect du code. Ces organismes peuvent être internes ou externes (en tant que comité *ad hoc*). Les exigences ci-après s'appliquent à tous les organismes de contrôle, qu'ils soient internes ou externes.

« L'autorité de contrôle » mentionnée dans le référentiel ci-après désigne la CNIL.

Exigences
1. Exigences générales
Note explicative : Ces exigences visent à établir un cadre général pour les activités de l'organisme de contrôle. Elles portent également sur les garanties qu'il devra fournir afin de démontrer la bonne gestion de ses activités ainsi que son indépendance financière et matérielle.
1.1 L'organisme de contrôle met en place une démarche visant à s'assurer que tous les traitements qu'il effectue dans le cadre de ses missions sont conformes au RGPD.
1.2 L'organisme de contrôle doit démontrer que toutes ses ressources humaines, financières et matérielles sont proportionnées au périmètre du code de conduite. Ces ressources sont adaptées au nombre, à la taille des adhérents ainsi qu'à la complexité ou au niveau de risque des traitements mis en œuvre par les adhérents.
1.3 Les obligations et les éléments essentiels de la fonction de l'organisme de contrôle sont prévus par le code de conduite.
1.4 L'organisme de contrôle s'assure que les documents liés à l'exercice de ses missions (documentation fournie, plan d'audit, preuves d'audit, rapport d'audit, etc.) sont conservés de manière à préserver leur confidentialité ou sont détruits définitivement et en toute sécurité s'ils ne sont plus utiles après la mission de contrôle (sous réserve d'autres obligations légales ou de raisons légitimes).
1.5 L'organisme de contrôle s'assure que dans le cadre de la réalisation de ses missions, les mesures de sécurité prévues par l'adhérent sont respectées par l'organisme de contrôle. Ces mesures de sécurité ne doivent pas empêcher l'organisme de contrôle d'exercer ses missions.
2. Exigences relatives à l'indépendance de l'organisme de contrôle

Exigences
Note explicative : L'indépendance d'un organisme de contrôle est garantie par la mise en place de règles et de procédures formelles encadrant sa désignation, son mandat et son fonctionnement. Dans le cadre de sa demande d'agrément auprès de l'autorité de contrôle, l'organisme de contrôle devra faire la démonstration de son indépendance fonctionnelle, matérielle et décisionnelle. Le respect de chaque exigence fera l'objet d'une évaluation au regard des justificatifs apportés. Les exigences et les exemples listés ci-après s'appliquent à l'organisme de contrôle, qu'il soit interne ou externe.
2.1 L'organisme de contrôle doit démontrer le principe de son indépendance, notamment vis-à-vis du porteur du code, des adhérents et des professionnels du secteur concerné.
2.2 L'organisme de contrôle doit démontrer son indépendance fonctionnelle vis-à-vis du porteur de code et des adhérents au code dans l'accomplissement de ses tâches et l'exercice de ses pouvoirs. L'organisme de contrôle doit disposer des ressources humaines et techniques nécessaires à l'exécution efficace de ses tâches. L'organisme de contrôle doit établir qu'il est ainsi en mesure d'exercer pleinement ses fonctions de contrôle, en tenant compte du secteur concerné et des risques liés aux activités de traitement visées par le code de conduite.
2.3 L'organisme de contrôle doit démontrer son indépendance financière en établissant qu'il dispose d'un financement et d'une viabilité financière suffisants pour accomplir ses tâches. L'organisme de contrôle doit démontrer que les règles relatives à son financement préviennent tout risque d'atteinte à son indépendance ou à l'exécution de ses tâches, notamment par un adhérent.
2.4 L'organisme de contrôle doit démontrer son indépendance au cours du processus décisionnel, y compris en ce qui concerne le choix de son personnel chargé des missions de contrôle.
2.5 L'organisme de contrôle doit établir qu'il est seul décisionnaire dans le cadre de ses activités de contrôle. Sans préjudice des missions et des pouvoirs de l'autorité de contrôle, les décisions prises par l'organisme de contrôle en rapport avec ses fonctions ne sont pas soumises à l'approbation d'un autre organisme, y compris le porteur de code.

Exigences
3. Exigences relatives à l'absence de conflit d'intérêts
Note explicative : L'absence de conflits d'intérêts est garantie par la mise en œuvre de mesures et de procédures visant à prévenir de telles situations.
3.1 L'organisme de contrôle doit rester à l'abri de toute influence extérieure, directe ou indirecte. Il ne doit ni solliciter ni accepter d'instructions provenant de personnes, d'organisations ou d'associations.
3.2 L'organisme de contrôle doit être en capacité d'identifier toute situation susceptible de créer un conflit d'intérêts (du fait de son personnel, de son organisation, de ses procédures, de ses sous-traitants, etc.)
3.3 L'organisme doit mettre en place des procédures et des mesures permettant d'éviter les conflits d'intérêts, de telle sorte qu'il s'abstienne de toute action incompatible avec ses tâches et ses fonctions. L'organisme de contrôle doit prévoir une procédure permettant de traiter toute situation susceptible de créer un conflit d'intérêts.
3.4 L'organisme de contrôle doit disposer de son propre personnel choisi par lui ou par un prestataire indépendant du code.
4. Exigences relatives à l'expertise de l'organisme de contrôle
Note explicative : Chaque demande d'agrément est évaluée *in concreto*, en tenant compte également des exigences d'expertise spécifiques définies par le code concerné. Les exigences en matière d'expertise sont définies en tenant compte de divers facteurs tels que le secteur d'activité concerné par le code de conduite, la taille de ce secteur, le nombre d'adhérents au code, les risques liés aux activités de traitement et les divers intérêts en jeu.
4.1 Exigences relatives au personnel de direction chargé du processus décisionnel
4.1.1 L'organisme de contrôle doit démontrer qu'il dispose des compétences nécessaires pour mener à bien les activités de contrôle du code concerné.
4.1.2 L'organisme de contrôle doit démontrer que le personnel chargé de prendre les décisions a une connaissance et une expérience approfondies des questions et enjeux relatifs à la protection des données et du secteur spécifique du code de conduite, ainsi qu'en ce qui concerne l'exercice de missions de contrôle. Ces compétences ne sont pas nécessairement réunies en une seule et même personne.
4.2 Exigences relatives au personnel exerçant les activités de contrôle

Exigences
4.2.1 Le personnel doit avoir suivi une formation sur les méthodes d'audit (principes, procédures et techniques d'audit, documents relatifs aux audits, règlements et autres exigences applicables en la matière, etc.).
4.2.2 Le personnel doit avoir participé à au moins deux audits complets, depuis leur préparation jusqu'aux conclusions finales, au cours des trois dernières années.
4.2.3 Le personnel doit pouvoir bénéficier d'un programme de formation professionnelle.
4.2.4 Le personnel doit avoir le niveau d'expertise requis en ce qui concerne les activités de traitement objet du code et une connaissance approfondie des questions de protection des données en rapport avec le secteur spécifique du code.
4.2.5 Le personnel doit avoir bénéficié d'une formation spécifique sur la protection des données à caractère personnel.
4.2.6 Le personnel ayant un profil juridique doit être titulaire *a minima* d'un master 1 ou d'un diplôme équivalent dans le domaine du droit.
4.2.7 Le personnel ayant un profil juridique doit avoir au moins deux ans d'expérience professionnelle dans le domaine de la protection des données à caractère personnel (par exemple, conseil, contentieux, etc.).
4.2.8 Le personnel ayant un profil technique est titulaire *a minima* d'un diplôme de licence ou équivalent dans le domaine de l'informatique, des systèmes d'information ou de la cybersécurité.
4.2.9 Le personnel ayant un profil technique a reçu une formation de deux jours au minimum sur les référentiels utiles au management de la sécurité des systèmes d'information (réglementation, normes, méthodes, bonnes pratiques, gestion des risques, etc.).
4.2.10 Le personnel ayant un profil technique a une expérience de deux ans au minimum dans le domaine de la sécurité des systèmes d'information.

Exigences
5. Exigences relatives aux procédures de l'organisme de contrôle
Note explicative : Ces exigences visent à garantir que les activités et missions de contrôle menées par l'organisme de contrôle sont régulières, complètes et transparentes pour l'adhérent au code de conduite. La procédure de contrôle peut être conçue de différentes manières, telles que des audits aléatoires et inopinés, des inspections annuelles, des rapports réguliers et l'utilisation de questionnaires. La procédure de contrôle mise en œuvre par l'organisme de contrôle doit être conforme au cadre établi par le code de conduite.
5.1 L'organisme de contrôle doit démontrer que la procédure de contrôle détermine les compétences nécessaires à l'exécution de la mission et garantit que le personnel possède les compétences requises pour exécuter la mission de contrôle.
5.2 L'organisme de contrôle doit démontrer que la procédure de contrôle comprend un engagement du personnel portant sur le respect des principes de déontologie, d'indépendance, de présentation impartiale des résultats et l'utilisation d'une approche méthodique.
5.3 L'organisme de contrôle doit démontrer que la procédure prévoit des contrôles réguliers, effectués d'une manière indépendante qui permettent : – d'évaluer l'éligibilité des responsables de traitement et/ou des sous-traitants à adhérer au code, – de contrôler le respect du code après l'adhésion, et – de procéder à l'évaluation du bon fonctionnement des différents mécanismes prévus par le code.
5.4 L'organisme de contrôle doit démontrer qu'il a mis en place un programme de contrôle tenant compte d'éléments tels que la complexité des traitements et les risques qui y sont associés, le nombre des adhérents au code, la portée géographique du code et les plaintes reçues.
5.5 L'organisme de contrôle doit démontrer que la procédure de contrôle garantit l'intégrité et la traçabilité des preuves lors de la collecte des informations nécessaires.
5.6 L'organisme de contrôle doit démontrer que les résultats et les conclusions du contrôle sont exposés et expliqués aux adhérents au code contrôlé, dans un délai raisonnable. Lors d'un contrôle, les remarques écrites ou orales faites par un adhérent à la réception des constatations et des conclusions sont énumérées dans le rapport.

6. Exigences relatives au traitement des plaintes

Note explicative :

L'organisme de contrôle met en place des procédures pour le traitement impartial et objectif des plaintes concernant les violations du code ou la manière dont le code est appliqué par un adhérent. Ces procédures sont transparentes et publiques à l'égard de tous.

La procédure de traitement des plaintes établie par l'organisme de contrôle permet de traiter les plaintes émanant d'un adhérent au code ou de toute personne pouvant démontrer un intérêt légitime. Le traitement des plaintes doit faire l'objet d'une affectation de ressources suffisantes et le personnel impliqué doit faire preuve de suffisamment de connaissances et d'impartialité.

Cette procédure est également basée sur le code de conduite applicable.

6.1 L'organisme de contrôle établit une procédure pour recevoir, gérer et traiter les plaintes. L'organisme de contrôle doit démontrer que cette procédure est impartiale et transparente.

6.2 Cette procédure doit être compréhensible et aisément accessible par tout public, y compris les personnes concernées et les adhérents au code.

6.3 L'organisme de contrôle veille à ce que toutes les plaintes soient traitées et fournit au plaignant des rapports sur l'état d'avancement de la procédure ou son résultat dans un délai raisonnable, par exemple trois mois, à compter de la réception de la plainte.

Le délai de résolution de la plainte peut être prolongé d'une durée raisonnable si nécessaire, en tenant compte de la complexité de la plainte. L'organisme de contrôle informe le plaignant de cette prolongation dans un délai de trois mois à compter de la réception de la plainte, en indiquant les raisons de la prolongation du délai.

6.4 L'organisme de contrôle tient un registre du traitement de toutes les plaintes reçues.

L'organisme de contrôle tient ce registre à la disposition de l'autorité de contrôle, qui peut y accéder à tout moment.

6.5 L'organisme de contrôle doit rendre ces décisions, ou les informations générales y afférentes, accessibles au public, conformément à sa procédure de traitement des plaintes.

Ces informations générales peuvent inclure, de façon non-exhaustive, des informations statistiques générales concernant le nombre et le type de plaintes/infractions et les résolutions/mesures correctives émises. Ces informations générales doivent comprendre les informations relatives aux sanctions qui ont entrainé la suspension ou l'exclusion d'un adhérent.

7. Exigences relatives à l'information de l'autorité de contrôle
Note explicative : Ces exigences détaillent les informations qu'un organisme de contrôle doit régulièrement communiquer à l'autorité de contrôle.
7.1 L'organisme de contrôle rassemble dans un seul document la synthèse de toutes les actions entreprises. Ce document est à la disposition de l'autorité de contrôle, qui peut y accéder à tout moment.
7.2 L'organisme de contrôle informe l'autorité de contrôle, sans délai et par écrit, de toute modification substantielle (notamment de structure ou d'organisation) susceptible de remettre en cause son indépendance, son expertise et l'absence de tout conflit d'intérêts.
7.3 L'organisme de contrôle informe l'autorité de contrôle, par écrit, lorsqu'une mesure contraignante est prise à l'encontre d'un des adhérents au code de conduite. Cette information inclut une présentation des motifs ayant justifié cette mesure. La fréquence des communications est basée sur plusieurs critères, dont la gravité de l'infraction et la mesure adoptée.
7.4 L'organisme de contrôle informe l'autorité de contrôle, sans délai et par écrit, dès que l'adhésion d'un adhérent du code de conduite est suspendue. Cette information inclut une présentation des motifs ayant justifié cette mesure.
7.5 L'organisme de contrôle informe l'autorité de contrôle, sans délai et par écrit, dès qu'un adhérent est exclu du code de conduite. Cette information inclut une présentation des motifs ayant justifié cette mesure.
8. Exigences relatives aux mécanismes de révision
Note explicative : Le porteur de code peut décider de modifier ou d'étendre la portée du code et/ou son contenu. Dans ce cas, des organismes de contrôle sont impliqués dans ce processus : ils jouent un rôle clé en contribuant à la mise à jour du code conformément aux mécanismes de révision prévus par le code de conduite.
8.1 L'organisme de contrôle contribue au réexamen et/ou aux modifications du code décidées par le porteur de code.
8.2 L'organisme de contrôle doit prévoir des procédures permettant d'intégrer et de mettre en œuvre le contrôle des modifications décidées par le porteur de code.
8.3 L'organisme de contrôle fournit également au porteur de code un rapport périodique sur le fonctionnement du code.
9. Exigences relatives au statut juridique
9.1 Exigences relatives à l'organisme de contrôle

9.1.1 L'organisme de contrôle est établi dans l'Union européenne.
9.1.2 L'organisme de contrôle est responsable, devant l'autorité de contrôle, de toutes ses actions et décisions liées à ses activités.
9.1.3 L'organisme de contrôle dispose de ressources financières, humaines et matérielles suffisantes et de procédures permettant d'assurer la continuité de ses activités de contrôle pendant toute la durée de l'agrément.
9.2 Exigences relatives à la gestion de la sous-traitance
Note explicative : L'objectif de ces exigences est de garantir le respect de ce référentiel d'agrément lorsque l'organisme de contrôle a recours aux services d'un sous-traitant pour l'exercice de ses missions de contrôle.
9.2.1 L'organisme de contrôle établit un contrat ou un autre acte juridique au titre du droit de l'Union européenne, le liant au sous-traitant de sorte que toutes les missions sous-traitées soient conformes au RGPD. Le recours à la sous-traitance n'entraine pas de délégation de responsabilité : dans tous les cas, l'organisme de contrôle reste responsable du contrôle du code de conduite devant l'autorité de contrôle.
9.2.2 L'organisme de contrôle s'assure que tout sous-traitant satisfait aux exigences du présent référentiel, notamment en ce qui concerne l'indépendance, l'absence de conflit d'intérêts et l'expertise.
9.2.3 L'organisme de contrôle prévoit l'insertion d'une clause particulière dans le contrat établi avec le (ou les) sous-traitant(s) afin de garantir la confidentialité des données à caractère personnel qui pourraient, le cas échéant, être portées à la connaissance du sous-traitant dans le cadre du contrôle.
10. Exigences relatives aux sanctions et mesures correctives décidées par l'organisme de contrôle
10.1 L'organisme de contrôle applique les mesures correctives et les sanctions prévues par le code de conduite.
10.2 L'organisme de contrôle doit s'assurer que, conformément au code de conduite, les droits de l'adhérent sont respectés lorsque l'organisme demande l'application de mesures correctives ou prononce des sanctions.