Article : RGPD - Codes de conduite et certification

Lignes directrices sur les codes de conduite et les annexes aux lignes directrices sur l'accréditation et la certification.

Le Comité Européen de la Protection des Données (CEPD) a publié, ce 14 juin 2019, la version finale de ses lignes directrices sur les codes de conduite et les organismes de contrôle accrédités ainsi que les annexes de celles relatives aux organismes accrédités pour la certification et les critères de certification. Ces dernières font échos au schéma de **certification CARPA** lancé en consultation publique par la CNPD en mai 2018.

Préambule

Pour rappel, l'art 40 stipule que l'élaboration des codes de conduites est destinée « *à contribuer à la bonne application du présent règlement, compte tenu de la spécificité des différents secteurs de traitement et des besoins spécifiques des micro, petites et moyennes entreprises*. » Tandis que l'art 41 dispose que le contrôle du respect de ces codes de conduites peut être effectuer *« par un organisme qui dispose d'un niveau d'expertise approprié au regard de l'objet du code et qui est agréé à cette fin par l'autorité de contrôle compétente.* » Il faut noter que cette accréditation ne concerne pas les organismes publics.
L'art 43 définit le rôle et les missions des organismes de certification, les critères d'agréement[1] étant laissés à l'appréciation par les autorités de contrôle ou par le CEPD.
Néanmoins, ces lignes directrices établissent un cadre clair pour toute autorité de contrôle compétente (*CompSA*).
Il est intéressant de noter que l'utilisation de codes de conduites et de la certification par des organismes accrédités se rapproche du concept de l'assurance qualité [2].

Codes de conduites

Le code de conduite est définit comme **un outil d'assurance de prise de responsabilité volontaire** (« *voluntary accountability tool* ») se référant aux exigences du RGPD (*ex. intérêts légitimes, pseudonymisation, exercices des droits des personnes concernées, mesures techniques et organisationnelles appropriées, gestion de la violation des données,…*) , à ses avantages (*ex. codes sectoriels applicables à un ensemble de PMEs et Micro entreprise*) et aux procédures d'admissibilité et d'approbation selon qu'il s'agisse de codes de conduite nationaux ou transnationaux.
Ces codes doivent contenir un certain nombre de mentions avant d'être soumis à l'autorité de contrôle compétente, notamment :

- Énoncé de mission
- Représentants
- Périmètre territorial et matériel
- Consultation préalable des acteurs du secteurs
- Références légales et réglementaires de l'état membre concerné
- La langue de communication

Des supports explicatifs sont fournis dans les annexes :

- Annexe 1 : définition des codes de conduite nationaux et transnationaux (*application dans plus qu'un état membre*)

- Annexes 2 : comment choisir l'autorité de contrôle compétente ?
- Annexe 3 : Liste de contrôle avant soumission

Les autorités de contrôle ne sont pas en reste. En effet, les critères d'approbation ainsi que les étapes de la procédure sont listés.

L'accréditation et la certification

[1] Voy art 43.3 : « *L'agrément des organismes de certification visés aux paragraphes 1 et 2 du présent article se fait sur la base de critères approuvés par l'autorité de contrôle qui est compétente en vertu de l'article 55 ou 56 ou, par le comité en vertu de l'article 63.* »

[2] Voy ISO 8402 : « *Ensemble des activités préétablies et systématiques mises en œuvre dans le cadre du système qualité, et démontrées en tant que besoin, pour donner la confiance appropriée en ce qu'une entité satisfera aux exigences pour la qualité.* »

Le CEPD, conscient de l'absence de définition claire de l'accréditation, a posé la description suivante : « *une attestation délivrée par un organisme national d'accréditation et/ou par une autorité de contrôle, de sorte que l'organisme certificateur reçoive l'agrément pour délivrer ladite certification conformément aux articles 42 et 43 du RGPD, en tenant compte des exigences de l'ISO/IEC 17065/2012 et des exigences complémentaires définies par l'autorité de contrôle et/ou le Comité* [3] . »
Par conséquent, l'accréditation peut être délivrée par un organisme autre que l'organisme national d'accréditation (*art43.1(b)*). C'est pourquoi, le comité considère que l'intention du législateur européen est de déroger au principe général, à savoir que seul l'organisme nationale d'accréditation accorde l'agrément, en octroyant ce pouvoir à l'autorité de contrôle.
Néanmoins, le comité note que l'autorité de contrôle « *procède à l'agréement d'un organisme de certification* » (*art 5.1(q)*). En outre, au regard de l'art 58.3 (e), l'autorité de contrôle dispose d'un pouvoir d'autorisation et d'un pouvoir consultatif pour « *agréer les organismes de certifications en application de l'art 43* ». Selon le comité, en raison de formulation souple de l'art 43, cette compétence résiduelle devrait être interprétée comme une mission uniquement lorsqu'elle est appropriée.
Les conditions d'accréditation pour l'organisme certificateur sont définies dans l'annexe 1 :

- Critères généraux : application de la norme ISO/IEC 17065/2012
- Critère(s) structurel(s) : laissé(s) à la libre appréciation de l'autorité de contrôle
- Critères humains : l'organisme doit démontrer l'expertise de son personnel dans les matières liées à la protection des données et spécifiquement sur le plan technique. Il doit aussi s'assurer à ce que cette activité n'entre pas en conflit d'autres.

Etude de cas : le grand-duché de Luxembourg et le schéma GDPR CARPA

Le mécanisme de certification CARPA[4] résultant des travaux de la CNPD comporte 2 piliers :

- Les critères de certification
- Les critères d'agrément

A. *Les critères de certifications*

Le schéma fait référence à 7 points d'exigences quelque soit le secteur ou le périmètre de la conformité :

1. Base légale du traitement (art 6- licéité)
2. Les principes (art 5)
3. Les droits des personnes concernées (art 12 à 23)
4. La notification en cas de violation de données (art 33)
5. Le privacy by design ou par défaut (art 25)
6. L'analyse d'impact (DPIA – art 35.7.d)
7. Les mesures techniques et organisationnelles appropriées (art 32 – CID)

Quels sont les avantages ?

- Le modèle accorde une certaine flexibilité au processus de certification. En effet l'organisme candidat à la certification peut fixer le périmètre en fonction de ses activités ou des traitements selon sa qualité (responsable de traitement et/ou sous-traitant).

- Le modèle fait état d'un niveau de granularité des composants ou facteurs influenceurs
  - Rôle : responsable de traitement /sous-traitant
  - Niveau 1 : type d'organisme (ex. *société privée, association, autorité publique*)
  - Niveau 2 : degré dans la hiérarchie organisationnelle (*ex. département, service*)
  - Niveau 3 : le niveau applicatif fonctionnel (*ex. ERP,CRM*)
  - Niveau 4 : infrastructure du système d'information (ex. OS, Cloud, DB server, Network Ad)

B. L'agrément

Le schéma GDPR-CARPA repose sur un **processus d'évaluation de l'organisme certificateur**, composé

[3] VOY (28): "*an attestation by a national accreditation body and/or by a supervisory authority, that a certification body is qualified to carry out certification pursuant to Article 42 and 43 GDPR, taking into account ISO/IEC 17065/2012 and the additional requirements established by the supervisory authority and or by the Board*."

[4] CARPA signifie Certified Assurance Report based Processing Activities

des étapes suivants :

- Audit sur base du référentiel GDPR-CARPA reprenant les points de l'annexe 1 des lignes directrices du CEPD
- L'analyse de l'argumentaire et/ou de la motivation de l'organisme candidat
- L'analyse des points de conformité (rencontre des critères précités)
- Décision d'octroi

Il est important de souligner que c'est la CNPD qui est l'organe accréditeur[5]

Conclusion

Comme le souligne l'APD de Belgique, « *Le code de conduite est un outil de conformité qui peut contribuer à démontrer le respect de certaines exigences du RGPD et considérablement faciliter la mise en conformité des petites et moyennes entreprises.* »[6]

[5] Voy Working draft –1stOctober 2018 : « Only CNPD is entitled to provide an accreditation for the GDPR –CARPA certification mechanism described in this document."

[6] Voy APD Belgique