

Article : RGPD - Codes de conduite et certification - Autriche

Le CEPD recale la version préliminaire des critères d'accréditation des organismes de contrôle de suivi des codes de conduites de l'autorité de contrôle autrichienne

Pour rappel, le législateur européen permet aux associations et organismes privés ou public d'élaborer des codes de conduites applicables à un ensemble d'entreprises actives dans un secteur, « *compte tenu des spécificités des traitements effectués dans certains secteurs et des besoins spécifiques des micro, petites et moyennes entreprises.* »¹. Le Règlement Général de Protection des données (ci-après « RGPD ») dispose en ses articles 40 et 41 les modalités d'applications indispensables, laissant aux états membres et à leur autorités de contrôle respectives le soin de les mettre en place. Le CEPD est notamment compétent pour rendre les avis suivants² sur les projets de codes de conduites :

- Vérifier que le projet de code de conduite soumis à approbation respecte les dispositions du RGPD.
- Approuver les critères d'agrément d'un organisme de contrôle de suivi des codes de conduites ou de certification

Le CEPD s'est prononcé récemment sur les critères d'agrément de l'autorité de contrôle autrichienne.³ Pour rendre son avis, le comité s'est basé sur ses propres lignes directrices publiées en février 2019 : Les conditions d'accréditation s'apprécient selon 8 critères⁴ :

- L'indépendance
- L'absence de conflits d'intérêts
- L'expertise
- Structures et procédures
- Procédure transparente de réclamation
- Communication avec l'autorité de contrôle compétente
- Mécanisme de révision
- Statut légal

Dans le cas d'espèce, les critères définis par l'autorité de contrôle autrichienne n'ont pas été estimés satisfaisants par le comité. En effet, l'indépendance et les conflits d'intérêts ne sont pas clairement établis. La procédure de réclamation n'est pas caractérisée sur base d'un processus spécifique incluant une transparence et une documentation effective.

Le CEPD pointe aussi l'absence de registre des plaintes et d'enregistrement des violations aux dispositions réglementaires, l'organisme de contrôle du suivi des codes de conduites contribuant activement aux mécanismes de révision. Mais le point le plus surprenant réside dans le fait que l'autorité de contrôle autrichienne permette à un organisme de contrôle établi à l'extérieur de l'EEE de recevoir cet agrément⁵ : un organisme de contrôle situé en Russie ou en Chine pourrait, par conséquent, approuver des codes de conduites d'une entreprise autrichienne sur base des dispositions du RGPD. Bien que le RGPD a un champ d'application extra territorial (*voir art 2.2*), il ne concerne que le traitement des données à caractère personnelle de personnes concernées et non du contenu de code de conduite applicable aux responsables

¹ Voy. [Considérant \(98\)](#) : « Il y a lieu d'encourager les associations ou autres organismes représentant des catégories de responsables du traitement ou de sous-traitants à élaborer des codes de conduite, dans les limites du présent règlement, de manière à en faciliter la bonne application, compte tenu des spécificités des traitements effectués dans certains secteurs et des besoins spécifiques des micro, petites et moyennes entreprises. Ces codes de conduite pourraient, en particulier, définir les obligations qui incombent aux responsables du traitement et aux sous-traitants, compte tenu du risque que le traitement peut engendrer pour les droits et libertés des personnes physiques. »

² Voy. [Art 64.1 \(b\) et \(C\)](#)

³ Voy [Opinion 9/2019](#) on the Austrian data protection supervisory authority draft accreditation requirements for a code of conduct monitoring body pursuant to article 41 GDPR , 12/07/2019 , EPDB

⁴ Voy. section 12, [Guidelines 1/2019](#) on Codes of Conduct and Monitoring Bodies under Regulation 2016/679,12/02/2019,EPDB

⁵ Voy, section [LEGAL STATUS](#): « The Board observes that section 2.2 of the AT SA's ordinance provides that a monitoring body **may be based outside of the EEA**. The Board is of the opinion that a monitoring body requires an establishment in the EEA. This is to ensure that they can uphold data subject rights, deal with complaints and that GDPR is enforceable and also ensures supervision by the CSA. The Board recommends that AT SA require that the monitoring body has an establishment in the EEA. »

Article : RGPD - Codes de conduite et certification - Autriche

de traitement et autres sous-traitants, à savoir « *définir les obligations qui incombent aux responsables du traitement et aux sous-traitants, compte tenu du risque que le traitement peut engendrer pour les droits et libertés des personnes physiques.*⁶ ».

En conclusion, le Comité recommande de revoir le projet sur base des points évoqués et selon le prescrit de l'art 64.4 et .8, de communiquer la décision de suivre ou non ladite opinion.

⁶ Voy. [Considérant \(98\)](#).