Newsletter Compliance

OCTOBRE 2021

Les dernières actualités de la compliance sélectionnées par le cabinet Vigo, à destination des compliances officers, DPO, responsables juridiques, auditeurs, ainsi que leurs relais de conformité internes.

***

SOMMAIRE

1. Compliance et devoir de vigilance 2
   - Amendement : devoir de vigilance et compétence du tribunal de commerce de Paris 2
   - Enquête de l'OCEG sur la performance des critères ESG 2
   - DGCCRF : rappel sur l'obligation de se doter d'une cartographie adaptée à l'activité de chaque professionnel. 2
   - La directive sur le devoir de vigilance se fait attendre 3
   - Loi Climat et Résilience : nouveautés autour du plan de vigilance 3
2. Protection des données à caractère personnel 4
   - Les nouvelles clauses contractuelles types (CCT) sont applicables depuis le 27 septembre 4
   - CNIL : 3.000 euros d'amende pour la société nouvelle de l'annuaire français (SNAF) 4
   - La CNIL lance une consultation sur un projet de Guide « Recrutement ». 5
   - RGPD : autoévaluation de maturité en gestion de la protection des données 5

1. COMPLIANCE ET DEVOIR DE VIGILANCE

- ***Amendement : devoir de vigilance et compétence du tribunal de commerce de Paris***

Le Projet de loi « Confiance dans l'institution judiciaire » a été amendé en première lecture par le Sénat afin de rendre compétent le tribunal de commerce de Paris pour connaître des litiges relatifs au devoir de vigilance « car son expertise et son organisation en font la juridiction la plus compétente pour appréhender une telle mission ».

Pour rappel, la compétence des tribunaux de commerce pour les actions relatives au devoir de vigilance (articles L. 225-102-4, II et L.225-102-5 du code de commerce) avait été reconnue par la cour d'appel de Versailles dans un arrêt du 10 décembre 2020.

Toutefois, l'amendement n'a pas obtenu l'avis favorable du gouvernement et le texte pourrait donc être à nouveau modifié par l'Assemblée nationale, qui penche pour la désignation d'une juridiction civile spécialisée.

Source 1

Source 2

- ***Enquête de l'OCEG sur la performance des critères ESG***

Le 13 septembre 2021, le groupe de réflexion Open Compliance and Ethics Group (OCEG) a publié un rapport relatif aux programmes environnementaux, sociétaux et de gouvernance (ESG) des entreprises. Si des efforts sont entrepris par les entreprises, force est de constater que des nombreux progrès restent à faire en la matière. À titre d'exemple, seulement 30% du panel indique avoir procédé à une évaluation du respect des critères ESG au cours de l'année passée. En outre, 28% des participants avouent ne pas être convaincus que leur société disposait de capacités ESG « matures et bien documentées », tandis que seulement 10% des personnes interrogées avouent avoir réellement confiance en leur performance ESG.

Ces chiffres démontrent que les critères ESG ne sont pas encore parfaitement assimilés par les sociétés. Ces dernières se doivent d'adopter une démarche proactive au regard des standards de plus en plus exigeants en la matière.

Source

- ***DGCCRF : rappel sur l'obligation de se doter d'une cartographie adaptée à l'activité de chaque professionnel.***

Si certaines sociétés sont soumises à la loi Sapin II et à l'obligation de se doter d'une cartographie des risques, d'autres sont assujetties à des exigences en matière de lutte contre le blanchiment.

En ce sens, une agence immobilière s'est vue sanctionnée par la DGCCRF en raison de plusieurs manquements à ses obligations en matière de lutte contre le blanchiment. Il lui est notamment reproché de ne pas avoir établi sa propre cartographie des risques, mais d'avoir seulement utilisé des fiches diffusées par le Syndicat National des Professionnels de l'Immobilier. Or, la DGCCRF rappelle que la cartographie des risques doit être adaptée à l'activité de chaque professionnel.

Le domaine d'intervention de l'AFA et de la DGCCRF diffère, mais il convient de constater qu'une convergence en matière de cartographie des risques se fait. Les sociétés soumises à cet exercice, peu importe le domaine, ont l'obligation de dresser une cartographie spécifique à leurs activités qui leur sont propres afin de lister les risques auxquels elles sont effectivement et réellement confrontées.

Source

- ***La directive sur le devoir de vigilance se fait attendre***

Initialement prévue pour le premier semestre de l'année 2021 puis décalée au mois de septembre, l'adoption du projet de directive européenne sur le devoir de vigilance est de nouveau retardée. La Commission européenne a annoncé une nouvelle date pour la fin du mois d'octobre.

Comme pour la loi n° 2017-399 du 27 mars 2017 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre, il semble que l'ambition affichée par l'Union européenne d'adopter une directive permettant d'instaurer un devoir de vigilance en matière de droits humains et environnementaux est freinée par le lobbying de certaines entreprises qui craignent une législation trop contraignante.

Il convient ainsi de rester vigilant et attentif à la sortie du texte afin de déterminer précisément son champ d'application et donc les sociétés qui seront concernées par ces nouvelles dispositions, ainsi que les nouvelles obligations mises en place.

Source

- ***Loi Climat et Résilience : nouveautés autour du plan de vigilance***

La loi n° 2021-1104 du 22 août 2021 portant lutte contre le dérèglement climatique et renforcement de la résilience face à ses effets, dite loi « Climat et Résilience » instaure deux nouvelles dispositions relatives au plan de vigilance.

Ainsi, à compter du 1er janvier 2024, le plan de vigilance des sociétés produisant ou commercialisant des produits issus de l'exploitation agricole ou forestière devra comporter des mesures propres à prévenir la déforestation associée à la production et au transport vers la France de biens et de services importés.

En outre, la loi crée une nouvelle conséquence au non-respect de l'obligation d'établir un plan de vigilance dans un cas spécifique. Désormais, une société qui n'est pas en mesure de présenter un plan de vigilance pour l'année qui précède l'année de publication de l'avis d'appel à la concurrence ou d'engagement de la consultation d'un marché public ou d'un contrat de concession sera susceptible d'être exclue de la procédure de passation de ce marché ou du contrat par l'acheteur ou l'autorité concédante.

Source

2. PROTECTION DES DONNEES A CARACTERE PERSONNEL

- ***Les nouvelles clauses contractuelles types (CCT) sont applicables depuis le 27 septembre***

Les clauses contractuelles types de la Commission européenne (ci-après « **CCT** »), permettant les transferts de données hors de l'Espace économique européen sur le fondement de l'article 46 du Règlement général sur la protection des données (ci-après « **RGPD** ») ont été mises à jour le 4 juin 2021 par une Décision 2021/914 de la Commission européenne.

Ces nouvelles CCT sont applicables depuis le 27 septembre 2021.

L'objectif de cette mise à jour est double : (1) tenir compte de l'entrée en vigueur du RGPD, et notamment pour prendre en compte des schémas de responsabilité plus complexes (chaîne de sous-traitance et co-responsabilité) mais également (2) tenir compte de la décision « Schrems II » de la Cour de justice de l'Union européenne.

En pratique :

- **Dès aujourd'hui** : les nouvelles CCT doivent être intégrées dans tous les nouveaux contrats impliquant un transfert de données hors de l'espace économique européen fondé sur les CCT.

  >> Revoyez vos modèles de contrat.

- **D'ici 15 mois** : les contrats en cours impliquant un transfert de données hors de l'espace économique européen fondé sur les CCT doivent être revus pour intégrer ces nouvelles CCT.

  >> À vos avenants !

Source

- ***CNIL : 3.000 euros d'amende pour la société nouvelle de l'annuaire français (SNAF)***

La CNIL a sanctionné, le 15 septembre 2021, la SNAF, éditrice du site internet annuairefrancais.fr, à la suite de plaintes indiquant des difficultés rencontrées lors de demandes d'effacement et de rectification de données à caractère personnel.

La CNIL a retenu les manquements suivants :

- Manquement à l'obligation de respecter les demandes de rectification des données dans le délai d'un mois (article 16 du RGD) ;
- Manquement à l'obligation de respecter les demandes d'effacement des données (article 17 du RGPD) ;
- Manquement à l'obligation de mettre en œuvre un registre des activités de traitement (article 30 du RGPD) ;
- Manquement à l'obligation de coopérer avec la CNIL.

Ce qu'il faut retenir :

- Les exigences du RGPD s'appliquent depuis 2018 à tous les organismes, quelle que soit leur taille (la SNAF est une TPE au capital social de 5.000 euros).
- Il est indispensable de mettre en place une procédure de respect des demandes d'exercice de droits des personnes concernées permettant de répondre aux demandes dans un délai d'un mois et de prévoir un registre de suivi pour répondre à l'obligation d'*accountability*.
- Le Registre des activités de traitement n'est pas optionnel !

Source 1

Source 2

- ***La CNIL lance une consultation sur un projet de Guide « Recrutement ».***

Le 20 septembre 2021, la CNIL a publié, dans une version ouverte à la consultation publique, un projet de Guide « Recrutement » à destination de tous les organismes.

Dans ce projet de guide, la CNIL vient notamment préciser les types de données qui peuvent être collectées dans le cadre du recrutement, la répartition des responsabilités entre les différents acteurs d'un processus de recrutement (agences d'intérim, recruteurs, employeur, etc.) ou encore les durées de conservation des données utilisées dans ce cadre.

Dans l'attente de la publication de la version définitive du Guide « Recrutement », ce projet peut être considéré comme le référentiel applicable pour la réalisation d'une analyse d'impact lorsque le traitement présente un « risque élevé » pour les candidats, par exemple lorsque le processus de recrutement implique l'utilisation d'un algorithme de sélection.

Le projet est soumis à consultation publique jusqu'au 19 novembre 2021 et la version définitive devrait être publiée en février 2022.

Source 1

Source 2

- ***RGPD : autoévaluation de maturité en gestion de la protection des données***

Depuis l'entrée en vigueur du RGPD, les exigences de conformité s'appliquent à tous les traitements et obligent les entreprises et organismes à mettre en œuvre des mécanismes et procédures internes pour démontrer le respect des règles relatives à la protection des données.

Grâce à l'outil d'autoévaluation publié par la CNIL le 9 septembre dernier, les organismes peuvent désormais appréhender et évaluer leur niveau de maturité dans l'exercice des 8 activités « génériques » liées à la protection des données.

5 niveaux de maturité sont prévus : ils correspondent à ceux définis dans l'ISO/IEC 21827 et le guide « maturité SSI » de l'ANSSI et sont gradués comme suit :

- Niveau 0 : pratique inexistante ou incomplète ;
- Niveau 1 : pratique informelle ;

- Niveau 2 : pratique répétable et suivi ;
- Niveau 3 : processus défini ;
- Niveau 4 : processus contrôlé ;
- Niveau 5 : processus continuellement optimisé.

En pratique :

Pour les organismes : Cette autoévaluation permet aux organismes de se positionner, de choisir quelles sont les actions à mener pour *in fine* améliorer la gestion de la protection des données traitées.

Pour les sous-traitants : L'outil d'autoévaluation de la CNIL peut également être utilisé par les organismes pour évaluer leurs sous-traitants afin de répondre à l'obligation à laquelle ils sont soumis par les articles 28 et 32 du RGPD.

En qualité de sous-traitant, les résultats de l'auto-évaluation peuvent également être présentés directement à vos clients afin de démontrer le respect de la réglementation.

Source 1

Source 2

Source 3