11 juillet 2018

Politique de gestion des risques
adoptée par la Commission de surveillance le 11 juillet 2018

Politique de gestion des risques

Plusieurs risques susceptibles d'affecter le fonctionnement de l'ADAGP ont été identifiés : fraudes internes ou externes attachées à la gestion des droits, atteinte à la sécurité informatique et atteinte à la protection des données à caractère personnel.

Pour appréhender efficacement ces risques, l'ADAGP mettra en œuvre les mesures concrètes définies ci-après.

1. Prévention des fraudes attachées à la gestion des droits

L'ADAGP procède, dans le cadre de son activité, à la perception et au versement de droits d'auteur. Elle doit veiller à ce que ces droits et l'ensemble des montants afférents (prélèvement statutaire, produits financiers) fassent l'objet d'un traitement exempt de toutes fraudes, qu'elles soient internes ou externes.

En janvier 2017, l'ADAGP s'interrogeait sur son niveau d'exposition aux risques de fraude et sur l'adéquation des procédures mises en place pour identifier ces risques et y répondre.

Elle a donc confié une mission complémentaire à son commissaire aux comptes qui s'inscrit dans le cadre de la Norme d'Exercice Professionnel 240 « Prise en compte de la possibilité de fraudes lors de l'audit des comptes ».

Cette mission a permis d'établir une cartographie des risques de fraude et un plan de prévention de ces risques.

■ En vue de prévenir et encadrer ces risques, l'ADAGP veillera à éviter toutes possibilités de :

- manipulation frauduleuse des comptes adhérents ;
- détournement de fonds et de moyens ;
- falsification d'information favorisant le montant de droits perçus ;
- vol de produits et d'informations sensibles ;
- fraude interne au sein des services.

■ L'ADAGP devra mettre en œuvre les mesures définies ci-après :

- Harmonisation et mise en cohérence des délégations et pouvoirs bancaires ;
- Encadrement des modifications des coordonnées de contact et des coordonnées bancaires des comptes adhérents ;
- Encadrement des moyens d'accès du système d'information ;

- Séparation des rôles entre les différentes entités en charge de la perception, de la répartition et du versement des droits ;
- Sensibilisation des collaborateurs au risque de fraudes internes et aux risques informatiques externes ;
- Organisation interne des tâches afin de limiter les risques de fraudes ;
- Contrôles des activités de répartition et de versement des droits.

■ L'ADAGP mettra en œuvre des moyens techniques efficaces pour mettre en œuvre ces mesures. Tout membre de la commission de surveillance pourra consulter le détail des mesures mise en œuvre pour chaque typologie de risques.

■ L'ADAGP procèdera à l'actualisation annuelle de la cartographie des risques de fraude et du plan de prévention de ces risques. Elle rendra compte annuellement à la commission de surveillance, lors de la réunion précédant l'assemblée générale ordinaire, de tout problème liée à la prévention des fraudes attachées à la gestion des droits qui aurait pu se présenter dans l'année écoulée.

2. Gestion des risques informatiques

Dans le cadre de ses activités, l'ADAGP utilise des systèmes d'information accessibles en interne et en externe. Pour faire face aux différentes menaces qui pèsent sur ces systèmes, l'ADAGP gère les risques informatiques en s'appuyant sur une politique de sécurité des systèmes d'information (PSSI).

La PSSI couvre l'ensemble des systèmes d'information de l'établissement avec toute la diversité que cela implique dans les usages, les lieux d'utilisation, les méthodes d'accès et les personnes concernées (salariés et intervenants externes).

Elle s'applique notamment :

- aux systèmes de gestion (comptabilité, application interne de gestion, système de paie),
- aux applications de messagerie, au stockage des données, aux sauvegardes, aux traitements des données, à la bureautique,
- aux systèmes de communication (réseaux, téléphonie, visioconférence),
- aux connexions avec d'autres systèmes externalisés,
- aux systèmes de reprographie (fax, imprimantes, copieurs),
- aux postes de travail.

Le besoin en sécurisation des Systèmes d'Information repose sur les critères suivants :

- la confidentialité,
- la disponibilité,
- l'intégrité,
- la non-répudiation,

L'analyse du degré de sensibilité des actifs informatiques (applications, données, matériels) couplée à l'analyse des risques, permet d'adapter le besoin et le niveau de protection nécessaire afin d'atténuer ou d'éliminer les risques informatiques.

Sous l'autorité de la direction générale, le pilotage courant de la PSSI est de la responsabilité du Responsable des Systèmes d'Information (RSI).

Son rôle est notamment de :

- proposer et faire évoluer la PSSI,
- faire connaître et faire appliquer la PSSI,
- établir avec le service juridique la charte informatique,
- participer aux projets de l'ADAGP,
- administrer les infrastructures en respectant les bonnes pratiques,
- s'assurer que les fichiers trace sont disponibles pour le recueil éventuel de preuve,
- sauvegarder les informations,
- établir un plan de reprise d'activité.

En cas de contournement de la PSSI par des salariés/intervenants externes de l'ADAGP, le RSI devra rappeler les règles d'utilisation des systèmes d'information. En cas de contournements répétés, la direction générale sera avertie afin de décider de la suite à donner pour mettre fin aux usages frauduleux.

En cas de détection d'intrusion dans les systèmes d'information de l'ADAGP, le service informatique sera mobilisé pour préserver les preuves et assistera le représentant légal pour déposer plainte auprès des autorités compétentes (SDLC/OCLCTIC – BEFTI - SCRC/C3N). Ces dernières pourront mandater des experts pour relever les indices nécessaires à l'enquête.

La réduction des risques s'inscrit dans une démarche d'amélioration continue. Les réponses apportées pour faire face aux différentes menaces, réduire les vulnérabilités et préserver l'activité de l'ADAGP, feront l'objet d'un rapport détaillé que tout membre de la commission de surveillance pourra consulter.

3. Protection des données à caractère personnel

Le Règlement européen n° 206/679 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, dit règlement général sur la protection des données (RGPD), est entré en vigueur le 25 mai 2018. Il a pour objet d'assurer un haut niveau de protection des données à caractère personnel, entendues comme toutes informations se rapportant à une personne vivante identifiée ou identifiable.

L'ADAGP procède, dans le cadre de son activité, au traitement de données à caractère personnel relatives 1° aux salariés de l'ADAGP, 2° aux auteurs vivants et aux ayants droit d'auteurs décédés, 3° aux personnes physiques amenées à échanger des informations avec l'ADAGP (utilisateurs, abonnés aux listes de diffusion…).

L'ADAGP doit veiller à ce que ces données fassent l'objet d'un traitement conforme à la loi et que des moyens appropriés soient mis en œuvre pour prévenir tout risque de divulgation à des tiers non autorisés.

Une protection inappropriée des données à caractère personnel peut causer un préjudice non seulement aux personnes concernées mais également à l'ADAGP, puisque la non-conformité aux prescriptions du RGPD peut être sanctionnée par des amendes administratives, dont le montant peut atteindre 20 millions d'euros ou 4% du chiffre d'affaires annuel de l'entreprise.

En vue de prévenir et encadrer ces risques, l'ADAGP devra mettre en œuvre les mesures définies ci-après :

■ L'ADAGP devra limiter les traitements de données à caractère personnel à ce qui est nécessaire à l'exercice de ses missions légales et statutaires. Elle devra veiller à ne communiquer aux organismes de gestion collective avec lesquels elle a conclu un accord de représentation (sociétés sœurs) que les données strictement nécessaires à la gestion des droits.

■ L'ADAGP mettra en œuvre des moyens techniques efficaces pour protéger les données à caractère personnel et en garantir l'intégrité.

■ L'ADAGP recensera de façon précise les traitements de données à caractère personnel auxquels elle procède, en distinguant selon les catégories de données, les objectifs poursuivis, les personnes qui traitent ces données et les flux de données depuis ou vers l'extérieur. Tout membre de la commission de surveillance pourra consulter le registre recensant ces traitements.

■ Bien qu'elle n'y soit pas tenue au regard de la nature des traitements de données mis en œuvre, l'ADAGP a choisi de désigner un délégué à la protection des droits (DPD) parmi les salariés de la société. Le délégué à la protection des droits assurera en toute indépendance une mission d'information et de conseil auprès du gérant et des services de la société, s'assurera du respect du RGPD et répondra aux demandes d'accès des membres, des salariés ou des tiers dont les données à caractère personnel sont traitées.

■ Le délégué à la protection des droits rendra compte annuellement à la commission de surveillance, lors de la réunion précédant l'assemblée générale ordinaire, de tout problème liée à la protection des données à caractère personnel qui aurait pu se présenter dans l'année écoulée.

■ En cas d'atteinte grave à la protection des données à caractère personnel traitées par l'ADAGP, le DPD devra informer sans délai la commission de surveillance de la nature de cette atteinte et des mesures mises en œuvre pour y remédier. De même, dans l'hypothèse où l'ADAGP serait saisie d'une demande de la Commission Nationale de l'Informatique et des Libertés (CNIL) relative à la mise en œuvre du RGPD, la commission de surveillance en sera informée.

La présente politique de gestion des risques prend effet immédiatement et restera en vigueur jusqu'à ce que la commission de surveillance en adopte une nouvelle.