# D7. Se prémunir des risques générés par les procédures de conformité (*compliance*)

La multiplication des réglementations juridiques et le renforcement de la culture de l'éthique ont conduit à la naissance d'une nouvelle matière mêlant management et droit : la **conformité** ou ***compliance***. Celle-ci a vocation à toucher tout le droit de l'entreprise. Et si elle peut paraître abstraite de prime abord, elle est bien concrète en ce qu'elle permet de gérer au mieux les risques de sécurité économique générés par l'activité de l'entreprise. En effet, l'essor de la conformité touche toutes les entreprises et toutes les branches du droit intéressant leurs activités. De manière générale, la conformité porte sur : la corruption, la fraude et le blanchiment, les pratiques anticoncurrentielles, les sanctions économiques (par exemple le contournement des embargos), la responsabilité sociale et environnementale des entreprises, la protection des données numériques, sans que cette liste soit limitative.

Le prononcé des sanctions est tout particulièrement important pour la sécurité économique des entreprises. En effet, un grand nombre d'États mettent en place des dispositifs de sanctions à portée **extraterritoriale** (les lois américaine et britannique telles que par exemple le ***Foreign Corrupt Practice Act*** et le ***UK Bribery Act***) pouvant sanctionner très lourdement des entreprises étrangères n'opérant pas sur leur territoire, notamment avec des amendes transactionnelles (comme les accords tel le **DPA** et **NPA**). Toutes les établissements, quelle que soit leur taille, étant concernés par ces dispositifs, doivent connaitre leur existence tant les conséquences peuvent être désastreuses. Pertes financières, perte de savoir-faire matériel et immatériel, perte de données stratégiques, dommage réputationnel, sanctions de mise en conformité avec imposition d'un **monitoring**, autant de risques pour la sécurité économique qu'une bonne compréhension de la *compliance* doit prévenir.

## Prévenir, grâce à des procédures internes

### ORGANISATIONNEL

➤ **Nommer un** ***responsable conformité***, qualifié et hiérarchiquement indépendant de la direction, qui coordonne les actions de prévention, de contrôle et de correction.

➤ **Rédiger une charte éthique** encadrant les comportements du personnel et la faire signer par tous.

➤ **Développer une veille** dédiée à l'activité législative et normative concernant l'activité de l'entreprise et son implantation géographique.

➤ **Sensibiliser** régulièrement les dirigeants comme les salariés aux bons comportements à adopter ainsi qu'aux risques encourus, tant pour l'entreprise que pour eux-mêmes, notamment en rappelant le cadre juridique s'appliquant aux cadeaux d'affaires.

➤ **Mettre en place un dispositif d'alerte** afin que le personnel puisse signaler au *responsable conformité* toute situation à risque ou suspecte. Les salariés doivent être informés de son existence et de la garantie d'anonymat qui leur est légalement accordée.

## Contrôler son organisation

### ORGANISATIONNEL

➤ **Vérifier systématiquement l'honorabilité** des partenaires et des tiers externes en se demandant si des éléments sont susceptibles de remettre en cause leur « bonne réputation » (sanctions, conflits d'intérêts, rumeurs défavorables, etc.) ?

➤ **Contrôler continuellement la conformité de son activité** aux normes juridiques, environnementales et éthiques applicables à l'entreprise et à ses implantations.

➤ Dresser **une cartographie des risques**, présentant des schémas de réponses concrets pour chacun d'eux et adaptés à la taille de l'entreprise et à son contexte local.

➤ **Conduire des audits** pour identifier et corriger les failles organisationnelles, comportementales et techniques pouvant motiver une procédure d'incrimination.

➤ En cas d'audits externes, veiller à **limiter les risques d'exposition du patrimoine informationnel de l'entreprise** : délimiter l'accès des sociétés étrangères aux ressources numériques, exiger la signature d'un accord de confidentialité et imposer le suivi de l'audit par un juriste interne.

### TECHNIQUE

➤ Veiller, dans la mesure du possible, à héberger et gérer les données propres au travers de solutions nationales agréées par l'Anssi.

### Mots clés

**Conformité (*compliance*) :** ensemble des processus qui permet d'assurer la conformité des comportements de l'entreprise, de ses dirigeants et de ses salariés aux normes juridiques et éthiques qui leur sont applicables.

**Extraterritorialité :** principe de droit international visant à laisser s'exercer dans un État l'autorité juridique d'un autre État.

***Foreign Corrupt Practice Act (FCPA) & UK Bribery Act*** : lois, respectivement des États-Unis et du Royaume-Uni, visant à sanctionner les actes de corruption. De portée extraterritoriale, ces législations peuvent s'appliquer à des acteurs étrangers ayant un lien quelconque avec l'État en question (États-Unis ou Royaume Uni selon la loi).

***Deferred Prosecution Act (DPA) :*** accord passé avec les autorités américaines ou britanniques par lequel une société, objet d'enquête pour corruption ou fraude, accepte de s'acquitter de sanctions financières, de reconnaître les faits et de se soumettre à un contrôle afin d'empêcher de futures infractions, en contrepartie de l'extinction des poursuites à son encontre.

***Non Prosecution Agreement (NPA)*** : négociation extra-judiciaire proposée à un établissement contre lequel il y a des soupçons de conduite déviante, mais contre lequel les autorités n'ont pas encore lancé de poursuites pénales.

**Monitoring** : technique visant à évaluer et contrôler le respect des engagements pris par une entreprise dans le cadre d'une transaction judiciaire (DPA ou NPA). Il peut être imposé à l'entreprise ou choisi par elle et est toujours financé par l'entreprise.

**Monitor :** personne désignée afin d'évaluer le respect des engagements pris par l'entreprise, son mandat est négocié entre l'entreprise et l'autorité de poursuite. Elle peut avoir accès à la quasi-intégralité des données de l'entreprise et peut potentiellement représenter un risque pour la sécurité économique de l'entreprise.

## D7. Se prémunir des risques générés par les procédures de conformité (suite)

**Pour aller plus loin**

Toutes concernées, les établissements doivent avoir conscience de la réglementation et notamment :

- la loi « Sapin II » sur la lutte anticorruption (annexe 2) ;
- le Règlement général sur la protection des données à caractère personnel (RGPD) expliqué sur le site de la Cnil.

- Anssi

Liste de produits certifiés de stockage sécurisé