# Confidentialité et loyauté

**Définition des concepts clés**

* **Confidentialité :**
* La confidentialité désigne l’obligation de protéger les informations sensibles ou stratégiques contre tout accès ou divulgation non autorisés. Elle s’applique tant aux documents physiques qu’aux données numériques. Dans le cadre professionnel, elle englobe :
	+ La restriction d’accès à certaines informations.
	+ L’établissement d’accords de confidentialité.
	+ Le respect des règles internes de l’entreprise concernant la gestion des données.
* **Loyauté :**
* La loyauté se réfère au comportement attendu de toutes les parties (salariés, partenaires, prestataires) pour agir de manière transparente, éthique et respectueuse des engagements contractuels. Cela implique de ne pas divulguer ou exploiter à des fins personnelles des informations obtenues dans un cadre professionnel.

**Cadre légal et sanctions en cas de non-respect**

En France, plusieurs lois encadrent la protection des informations sensibles, établissant des sanctions en cas de violation :

1. **Code pénal** :
	* **Abus de confiance (Article 314-1)** : Le détournement d’informations sensibles peut entraîner jusqu’à 3 ans de prison et 375 000 € d’amende.
	* **Atteinte au secret des affaires (Loi du 30 juillet 2018)** : Toute divulgation ou exploitation d’un secret d'affaires sans autorisation est passible de sanctions civiles et pénales.
2. **Code de la propriété intellectuelle** :
	* **Violation des droits d’auteur (Article L335-2)** : La reproduction ou la diffusion non autorisée de créations protégées peut être punie de 3 ans de prison et 300 000 € d’amende.
3. **Règlement Général sur la Protection des Données (RGPD)** :
	* **Non-respect de la confidentialité des données personnelles** : Les entreprises s’exposent à des amendes pouvant atteindre 20 millions d’euros ou 4 % de leur chiffre d’affaires annuel mondial.
4. **Code du travail** :
	* En cas de manquement d’un salarié à ses obligations de confidentialité ou de loyauté, des sanctions disciplinaires pouvant aller jusqu’au licenciement pour faute grave sont possibles.

**1. Identification et classification des informations sensibles**

**1.1. Recenser et catégoriser les informations**

Les entreprises doivent d’abord recenser les informations sensibles pour mieux les protéger. Cela inclut :

* **Données techniques et commerciales** : Prototypes, savoir-faire, stratégies marketing.
* **Données financières et stratégiques** : Offres commerciales, projets de fusion, budgets.

**1.2. Signalisation des informations sensibles**

Il est recommandé de marquer les documents contenant des informations critiques avec des mentions explicites telles que « Confidentiel » ou « Réservé ».

**2. Preuve de détention des informations : Dépôts privés**

**2.1. L’enveloppe Soleau**

Disponible auprès de l’INPI, cette méthode permet de dater officiellement un document.

**2.2. Dépôts notariés ou auprès d’huissiers**

Ces dépôts garantissent une preuve légale de la détention d’une information ou d’un savoir-faire à une date donnée.

**3. Implication du personnel et sécurisation des systèmes d’information**

**3.1. Sensibilisation des employés**

* **Formations régulières** sur la protection des données.
* **Signatures d’accords de confidentialité** avec tous les collaborateurs.

**3.2. Sécurisation informatique**

* Mise en place de pare-feu, systèmes de chiffrement et politiques d’accès restreint.

**4. Protection des informations par des accords de confidentialité**

Avant tout échange, un accord doit préciser :

* Les informations couvertes.
* Les responsabilités des parties.
* La durée de l’engagement de confidentialité.

**5. Innovations : Brevets et savoir-faire**

**5.1. Le brevet**

Protège les inventions pour une durée de 20 ans, offrant un monopole d’exploitation.

**5.2. Le savoir-faire**

Protégé par des engagements contractuels et la confidentialité, il reste non breveté mais stratégique.

**6. Confidentialité des offres et marchés publics**

**6.1. Marquer les documents sensibles**

Mentionner explicitement la confidentialité dans les documents d’appel d’offres.

**6.2. Respecter les cadres légaux**

Comprendre les lois relatives à la gestion des marchés publics pour éviter des fuites d’informations.

**Conclusion**

La protection des informations sensibles repose sur des pratiques rigoureuses, un cadre légal bien défini et la sensibilisation des parties prenantes. En respectant les principes de confidentialité et de loyauté, les entreprises peuvent réduire les risques de fuites d’information, protéger leur compétitivité et préserver leur image sur le marché.