

## **Eléments de recommandations à destinations des pôles de compétitivité et entreprises participant à des missions de partenariat technologique à l'étranger**

Afin d'accompagner les pôles de compétitivité et leurs membres dans leurs démarches de développement international (participation à des missions à l'étranger en vue de développer des partenariats technologiques avec des structures équivalentes du type « clusters » ou des entreprises), le Service de Coordination à l'Intelligence économique a rédigé des recommandations en vue de les sensibiliser à la nécessité d'identifier et de protéger leurs informations stratégiques.

Ce document, qui est amené à évoluer en s'enrichissant progressivement des retours d'expérience, n'aborde pas les aspects de la propriété intellectuelle, lesquels sont notamment traités dans le [Guide de la propriété intellectuelle dans les pôles de compétitivité](#). Ce guide, élaboré à l'initiative de la DRIRE Lorraine en partenariat avec le cabinet d'avocats Alain Bensoussan, permet aux animateurs et responsables des pôles de compétitivité d'acquérir de bons réflexes, d'instaurer des bonnes pratiques, de sensibiliser les partenaires engagés dans des projets collaboratifs et de les aider à organiser et sécuriser la propriété intellectuelle de leurs innovations.

## Recommandation n°1 : Préparation et protection des documents et données emportés lors des missions.

**Constats :** 1/ les cadres se déplacent avec leur ordinateur portable, leurs assistants numériques ... qui contiennent un ensemble de données qui peuvent être sensibles ou dont la compilation ou le regroupement en accroît le caractère sensible

et 2/ Les pertes et vols de matériels, les piratages, croissent parallèlement au taux d'équipement des entreprises.

**=> 3 précautions à prendre :**

**a. N'emmener avec soi que les documents / données qui sont strictement NECESSAIRES à la mission considérée.**

- Emporter uniquement les pièces d'identité et documents administratifs nécessaires, tout document (carnet d'adresses, agenda, notes, badge, papier à en-tête de la société, etc.) pouvant être volé ou dupliqué.
- N'emporter que les données pertinentes (ne pas prendre d'autres références, de traces d'autres négociations, de documents préparatoires à la mission...).
- Déterminer préalablement le niveau de sensibilité de ces données ; elles ne devront pas être placées sur le même support, avec le même dispositif d'accès (ordinateur portable, disque amovible, clé USB, enveloppe papier...).
- Laisser dans l'entreprise avant le départ une sauvegarde de l'ensemble des documents emportés.

**b. PROTÉGER les documents emportés en mission.**

→ Protéger l'ordinateur portable :

- utiliser un mot de passe complexe mêlant caractères numériques et alphabétiques (minuscules et majuscules) et le renouveler régulièrement (chaque trimestre par exemple) ; le modifier également avant le départ
- utiliser une sacoche discrète / anodine pour le transport du portable.

→ Placer / copier les fichiers les plus sensibles sur des périphériques amovibles (clés cryptées, CD Rom) plutôt que sur le disque dur de l'ordinateur.

Dans le cas où il n'est pas possible de placer les fichiers stratégiques sur des périphériques amovibles, alors il convient de les coder / crypter sur le disque dur de l'ordinateur portable à l'aide d'une clef complexe (utilisation de logiciels gratuits comme AxCrypt).

→ Ne pas se séparer de son ordinateur portable (exemples : ne pas le mettre à disposition pour effectuer une présentation : risque de copie via une clé USB en quelques secondes ; ne pas le laisser dans la salle de travail durant les pauses...).

→ Ne pas brancher sur son ordinateur une clé USB dont l'origine n'est pas parfaitement connue (risques que la clé soit infectée et contienne des dispositifs d'aspiration de fichiers, chevaux de « Troie »...).

→ Ne pas écrire ses mots de passe sur des documents papier, susceptibles d'être égarés.

→ Ne jamais laisser de documents confidentiels sans surveillance dans un lieu public même quelques minutes.

→ Ne pas laisser de documents ultraconfidentiels ni dans sa chambre d'hôtel, ni dans le coffre fort de l'hôtel ; les conserver avec soi.

→ Ne pas laisser un éventuel futur partenaire choisir et réserver pour vous l'hôtel. Changer régulièrement d'hôtel si plusieurs déplacements se succèdent dans une même localité.

**c. SAVOIR** que, vers certaines destinations, les portables + clés USB... peuvent être « fouillés<sup>1</sup> » en quelques secondes lors des contrôles pratiqués à l'entrée du pays.

→ Ne pas mettre sur l'ordinateur portable des documents que l'on ne souhaiterait pas « partager » (risques potentiels d'aspiration des disques durs ; NB : il est possible de reconstituer les données effacées préalablement dans le cadre de l'historique d'une négociation par exemple). Il vaut mieux par conséquent prendre un PC vierge.

---

<sup>1</sup> Des copies peuvent alors être effectuées à votre insu.

## Recommandations n°2 : Règles à suivre en matière de « communication ».

a. **Etre vigilant** sur les informations diffusées dans des **espaces publics** (salons, séminaires, cocktails, transports, restaurants, hôtels...) pour éviter des fuites qui pourraient se révéler préjudiciables pour l'entreprise.

**Comportements à éviter (risques de captation d'informations stratégiques)** : faire le compte-rendu d'un entretien par téléphone ou le taper sur son ordinateur portable dans un transport en commun, dans un salon d'aéroport, réaliser le *débriefing* avec ses collaborateurs de la participation à un salon dans un restaurant proche de l'événement...

Dans un espace public, il vaut mieux :

- Travailler uniquement sur des documents non confidentiels et utiliser des filtres rendant l'écran opaque ;
- Désactiver tous les moyens de communication offerts par votre portable (ports infrarouges, Wifi, Bluetooth...); s'il n'est pas possible de désactiver, alors lancer un logiciel détecteur d'intrusions (type *firewall*)
- Mettre à jour des correctifs de sécurité avant de le reconnecter sur le réseau de l'entreprise...
- Ne pas penser que la pratique du français dans un pays de langue étrangère permette de s'affranchir des règles de prudence à observer dans un espace public, mais également en présence de partenaires étrangers ;
- Ne pas aborder de sujets confidentiels ;
- Soyez vigilant si l'on vous invite à des confidences « *off the record* »

### b. Le cas d'une participation à un SALON.

#### → Avant le salon :

- Définir les informations qui pourront ou non être diffusées sur le salon ;
- Identifier les besoins d'informations et définir la façon de les obtenir (rencontre sur le stand avec le partenaire / concurrent, acquisition de plaquettes de communication, participation à une présentation organisée sur le salon ...);
- Etudier la disposition du salon, la place des exposants (concurrents, prestataires...), les opérateurs présents et ceux qui ne le sont pas (pourquoi ?) ;
- Limiter au strict minimum le nombre de documents ou matériels sensibles ;
- Préparer les axes de réponses sur les sujets liés au savoir-faire de l'entreprise (technologie, tour de main, innovations...).

#### → Pendant le salon :

- Ne pas laisser sans surveillance les matériels à risque (prototypes, maquettes...) et conserver les informations sensibles avec soi ;
- Profiter du salon pour collecter des informations stratégiques (prises de notes, plaquettes, rencontres...);
- Eviter les entretiens dans les lieux trop publics si vous souhaitez conserver une certaine discrétion ;
- Faire preuve de discrétion au restaurant et à l'hôtel où séjournent peut-être d'autres exposants ;
- Face aux visiteurs, s'assurer au mieux de son identité (carte de visite bilingue) ; faire attention aux concurrents anonymes ou aux « faux » journalistes ;
- Ne pas laisser de documents sensibles sur le stand même quelques instants ;
- Lors de la clôture, faire place nette sur le stand et vérifier l'ensemble des matériels et documents.

#### → Après le salon :

- Suivre les réactions d'après salon auprès du réseau commercial dans la presse ou sur internet ;
- Etablir un rapport de visite qui répertorie les informations stratégiques collectées (nouveaux contacts, informations techniques sur des produits, nouveaux matériaux...) et le diffuser aux collaborateurs concernés.

**Recommandation n°3 : Connaître les codes de négociation pratiqués dans le pays où s'effectue la mission.**

Les coutumes, les mentalités et les codes de négociations sont souvent très différents de ceux auxquels un homme d'affaires français, même des plus aguerris, peut être habitué.

Ne pas les connaître peut nuire à l'efficacité d'un déplacement à l'étranger.

Le réseau des services économiques à l'étranger de la Direction Générale du Trésor et de la Politique Economique ([www.dgtpe.fr/se/](http://www.dgtpe.fr/se/)) ainsi qu'Ubifrance, l'Agence française pour le développement international des entreprises ([www.ubifrance.fr/](http://www.ubifrance.fr/)), sauront apporter les éléments et les précisions sur les différents codes de négociation selon les différents pays.