



MINISTÈRE
DE L'AGRICULTURE,
DE L'AGRO-ALIMENTAIRE
ET DE LA SOUVERAINETÉ
ALIMENTAIRE

*Liberté
Égalité
Fraternité*



FranceAgriMer

ÉTABLISSEMENT NATIONAL
DES PRODUITS DE L'AGRICULTURE ET DE LA MER

Bonnes pratiques d'accueil de délégations étrangères

À destination des entreprises



Sommaire

Risques encourus lors de l'accueil de délégations étrangères	3
En amont de la visite	4
Pendant la visite	5
Après la visite	7
Fiche réflexe Informations sensibles	8
Fiche réflexe Demande d'information d'une autorité étrangère	9
Fiche réflexe Photos Enregistrements	10
Fiche réflexe Sécurité informatique	11
Fiche réflexe Interprétariat	12
Fiche réflexe Que faire en cas d'incident ?	13
Pour les industries agro-alimentaires	14

Risques encourus lors de l'accueil de délégations étrangères

La réalisation d'audits de conformité est un élément courant de la vie économique de l'entreprise. Ces audits favorisent néanmoins des situations de vulnérabilité et de fragilisation.



Risques de sécurité économique

- Collecte d'informations sensibles par les visiteurs (espionnage économique, fuite de données stratégiques).
- Accès inapproprié à des zones ou documents confidentiels.
- Photographies ou enregistrements non autorisés.



Risques juridiques

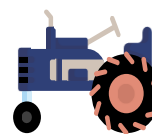
- Transmission de documents ou d'informations sensibles en violation de la loi de blocage (loi n° 68-678 du 26 juillet 1968).
- Engagement involontaire de l'entreprise dans des obligations légales étrangères.



Risques d'image et de relations internationales

- Manque de préparation pouvant donner une image négative de l'entreprise.
- Incompréhensions culturelles ou erreurs protocolaires.
- Perte de marchés à l'export.

En amont de la visite



Identifier les informations sensibles

- Définir les **informations sensibles** de l'entreprise (données, procédés, équipements...)
- Protéger l'accès aux informations sensibles physiquement et virtuellement

Anticiper la visite

- Connaître la composition de la délégation, l'identité complète et les titres professionnels des personnes et leur structure d'appartenance. Leur identité peut être complétée par un CV.
- Définir les **objectifs et enjeux de la visite** pour l'entreprise
- Établir un **itinéraire de visite non sensible** (itinéraire de courtoisie)
- Informer les salariés des dates et horaires ainsi que des précautions à prendre

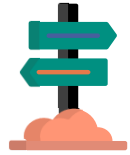
Préparer une présentation ciblée

- Préparer une **présentation de 20 à 30 min** sur l'entreprise visant les objectifs et enjeux pour l'entreprise
 - Présenter **succinctement l'entreprise** à laquelle appartient le site (groupe) et ses activités sans retracer tout l'historique de l'entreprise,
 - Présenter **l'organisation et fonctionnement du site** (année de construction, capacité, organisation des lignes de fabrication, derniers agrandissements, projets de travaux...).
 - Cibler les activités d'**export** : produits et volumes exportés vers le pays concerné et d'autres destinations.
 - Ne pas élargir la présentation en dehors de l'établissement ou de son agrément.
 - Présenter et valider le **circuit de visite** avec les auditeurs

Organiser la réception de la délégation

- Prévoir une **salle de réunion de taille adaptée** à la délégation, les interprètes et les accompagnants officiels (DGAL, FAM, DD(CS)PP) le cas échéant,
- **Regrouper les personnes** selon leur pays et fonction.
- Placer l'interprète à proximité de la délégation avec suffisamment de place pour les documents et qu'une personne de l'entreprise puisse s'approcher pour expliquer certains points. Le responsable qualité de l'entreprise sera placé à proximité de l'accompagnateur FAM pour échanger sur les réponses à apporter.
- Prévoir des **chevalets avec les noms des personnes**, en français et dans la langue des auditeurs (ou à défaut en anglais), **idéalement de couleur** selon la structure d'appartenance.
- Prévoir un **accès internet pour les visiteurs** indépendant de l'accès au réseau de l'entreprise (accès Expadon 2, listes établissements agréés).
- **Mettre à disposition des boissons chaudes** (café, thé, eau chaude), éventuellement des fruits, gâteaux.
- **Nettoyer** (tondre la pelouse) et **ranger** aux abords du site (éviter le stockage du vieux matériel non utilisé, identifier et protéger les zones de travaux)

Pendant la visite



Accueil

- Veiller à ce que les **abords du site soient bien sécurisés** (barrière baissée, portail fermé)
- Possibilité de dresser un drapeau du pays de la délégation en plus du drapeau français et européen

Installation

- Accueillir les auditeurs dans un espace dédié, avec un accès contrôlé aux autres locaux,
- Commencer par un tour de table des participants
- Donner la possibilité au responsable de la délégation d'exprimer ses attentes
- Présenter et sensibiliser les personnes aux règles d'accès et de sécurité dans l'entreprise

Photos et enregistrements

- Anticiper et encadrer la prise de photos et d'enregistrements

Visite

- Suivre le circuit de visite préétabli
- Prévoir un nombre d'accompagnants proportionné à la taille de la délégation. Toujours avoir un serre-fil qui passe en dernier et un ou plusieurs accompagnants pour les demandes individuelles (vestiaires, sanitaires...)
- Veiller à ce que la délégation reste groupée.
- Surveiller les demandes insistantes hors champ de l'audit ou les « électrons libres »
- Signaler toute demande ou incident aux accompagnants officiels

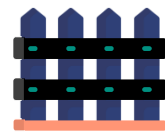
Échanges en salle

- Veiller à ce que toutes les communications passent par un **interprète qualifié** y compris pour l'anglais ou l'espagnol.
- Répondre aux questions de manière factuelle et concise, sans divulguer d'informations non demandées. En cas de question fermée, répondre par oui ou non et ne compléter que si cela est demandé.
- Laisser la personne la plus apte à répondre prendre la parole. Veiller à ne pas répondre à la place des services de contrôle.
- En cas de doute ou d'incompréhension, ne pas hésiter à faire répéter, préciser la question ou réexpliquer, reformuler la réponse jusqu'à avoir ou être compris.
- Ne pas laisser repartir les auditeurs sans les questionner sur leurs conclusions lors du **débriefing** avec des questions ouvertes du type : « Quels sont les points à problème ou qui nécessiteraient des améliorations que vous avez notés ? »

Documents

- L'établissement a à disposition le **plan de maîtrise sanitaire**.
- Prévoir **l'impression dans un format lisible** et si possible en couleurs des documents majeurs (quelques exemplaires en français et d'autres en anglais pour que tout le monde puisse suivre) : plan de l'établissement, circuit du personnel, circuit des produits, diagramme de production, résumé sur une page du plan HACCP...
- Les **comptes rendus des audits internes** et les **rapports d'inspection** des services vétérinaires doivent être à disposition des auditeurs.
- Uniquement les **notes de service DGAL** spécifiques pour l'export.
- Lorsque le pays tiers a des exigences spécifiques pour l'exportation, les documents précisant ces exigences pourront être regroupés dans un **classeur dédié** (possibilité aussi de les faire figurer sous la forme d'une liste de correspondance avec la réglementation CE).
- **Fournir les documents en version papier ou sur un support sécurisé** (USB préparée à l'avance).
- Proposer d'expliquer les documents présentés pour que les inspecteurs limitent leurs demandes de traduction. Faire une offre de transmission ultérieure si un document est vraiment exigé et n'est pas disponible.

Après la visite



Réaliser un débriefing en interne

- pour évaluer les échanges
- pour identifier d'éventuels risques encourus.

Conserver

- Copie des informations transmises
- Enregistrer les questions posées

Signaler

- Tout incident ou comportement suspect
- Assurer une veille auprès des concurrents

Contacts utiles

- **SHFDS (Service Haut fonctionnaire de défense et de sécurité du ministère en charge de l'agriculture) :** l-sg-shfds@agriculture.gouv.fr
- **CMDSZ (chef de mission défense et sécurité de zone) :**
 - Draafzone.est@agriculture.gouv.fr (Bourgogne Franche Comté, Grand Est)
 - Draafzone.ouest@agriculture.gouv.fr (Centre Val-de-Loire, Bretagne, Normandie, Pays-de-la-Loire)
 - Draafzone.sud@agriculture.gouv.fr (Provence-Alpes-Côte d'Azur, Occitanie, Corse)
 - Draafzone.sudest@agriculture.gouv.fr (Auvergne, Rhône-Alpes)
 - Draafzone.sudouest@agriculture.gouv.fr (Nouvelle-Aquitaine)
 - Draafzone.paris@agriculture.gouv.fr (Ile-de-France)
 - Draafzone.nord@agriculture.gouv.fr (Hauts-de-France)
- **SISSE (Service de l'information stratégique et de la sécurité économique) :** guichet.sisse@finances.gouv.fr
- **Référents régionaux DISSE :** <https://www.entreprises.gouv.fr/espace-entreprises/etre-accompagne/annuaire-des-disse-en-region>
- **Sécurité économique - Ministère de l'Intérieur :** securite-economique@interieur.gouv.fr

Fiche réflexe

Informations sensibles

Les entreprises manient quantité de données à la sensibilité inégale et évolutive. Seule une partie des données sera considérée comme sensible pour l'entreprise et parmi ces données seule une partie encore plus restreinte sera problématique pour l'entreprise et pour l'Etat

Pour en savoir plus...

Donnée sensible entreprise

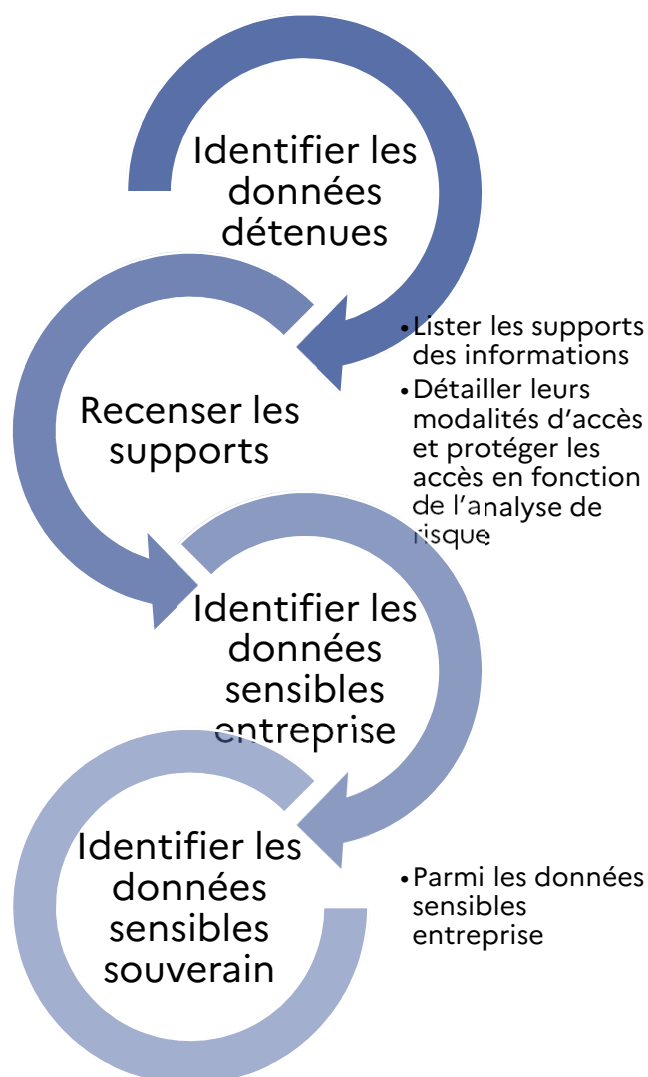
- Confidentialité : sa divulgation porte atteinte à l'entreprise
- Disponibilité : son indisponibilité porte atteinte à l'entreprise
- Intégrité : son altération porte atteinte à l'entreprise
- Toutes les données dont la communication à une autorité étrangère cause un préjudice grave à l'entreprise

Donnée sensible souveraine

- Leur communication porterait atteinte à la souveraineté, à la sécurité, aux intérêts économiques essentiels de la France ou à l'ordre public

Quelles données sensibles ?

- Économiques :
 - Plans de développement, projets d'innovation, décisions internes confidentielles
- Commerciales :
 - Contrats, conditions de négociation, listes clients, listes fournisseurs, intermédiaires.
- Industrielles et techniques :
 - Brevets, secrets industriels, codes sources, prototypes.
 - procédés de fabrication, recettes.
- Financières :
 - états comptables, investissements, coûts de production, marges bénéficiaires.



Fiche réflexe

Demande étrangère d'informations

L'entreprise est confrontée à une demande de communications par une autorité publique étrangère dans le cadre d'une procédure administrative ou judiciaire tel qu'un audit ou enregistrement de produits ou d'activité.

Cette demande couvre des informations identifiées comme sensibles.

Notification
immédiate

- Dès réception d'une demande étrangère, informez sans délai le SISSE : guichet.sisse@finances.gouv.fr
- Ce service est votre interlocuteur privilégié pour vous guider tout au long du processus.
- Cette saisine obligatoire opposable aux autorités étrangères protège l'entreprise

Accompagne-
ment
personnalisé

- Le SISSE vous fournira un accompagnement sur mesure, en lien avec les différentes administrations de l'État, pour vous aider à répondre aux demandes tout en respectant la loi de blocage.

Avis
administratif

- Vous recevrez un avis traduit en anglais de l'administration dans un délai adapté aux procédures judiciaires et administratives en cours.
- Cet avis renforcera l'opposabilité de la loi de blocage face aux juridictions étrangères.

Protection des
données

- Réduction de l'incertitude juridique
- Grâce à l'appui du SISSE, vous minimiserez les risques juridiques et assurerez une gestion sécurisée des demandes étrangères.



Protégez les intérêts de votre entreprise

- La loi de blocage de 1968 protège les informations sensibles de votre entreprise contre les demandes étrangères.
- Elle offre une **sécurité juridique renforcée** et un soutien administratif pour une meilleure protection juridique.



Répondez en toute confiance aux demandes étrangères

- Suivez les étapes avec le soutien du SISSE pour gérer les demandes étrangères en toute sécurité.



Évitez les sanctions

- Le non-respect de la loi peut entraîner des sanctions. Restez conforme pour éviter les pénalités.



Fiche réflexe

Photos Enregistre- ments

Les demandes de prise de photos sont très fréquentes, des enregistrements des échanges peuvent également être demandés. Il est en général mal perçu par les auditeurs d'interdire complètement la prise de photographies, mais des restrictions sont bien acceptées si elles sont définies et explicitées.

Ces mesures ne sont pas discriminatoires, elles ont vocation à être appliquées pour l'ensemble des délégations.

Respecter le droit à l'image

- Expliquer le principe du **droit des personnes concernant leur image**
- Éviter de prendre en photo les visages des employés pendant les visites
- Pour les enregistrements, préciser à tous les intervenants les phases d'enregistrement en cours et recueillir leur consentement

Interdire les photographies de certaines zones ou matériel

- Mettre en place une **signalétique visible pour interdire la captation** d'images dans les zones sensibles.
- Expliquer les restrictions et indiquer les zones à ne pas photographier au cours de la visite
- Désigner un accompagnateur chargé de veiller au respect des règles.

Proposer un service de prise de photos

- Prévoir qu'une responsable de l'entreprise prenne les photos à la demande des auditeurs au cours de la visite
- Les photos prises sont ensuite copiées sur un support informatique et remis aux auditeurs.

Vérifier

- Demander à visionner toutes les photos prises en cours de visite et effacer celles qui ne conviennent pas
- A noter l'intérêt de transmettre les photos prises aux accompagnants officiels DDPP, DGAL et FAM, en particulier celles concernant les anomalies relevées, car cela facilite la compréhension et les discussions les concernant, ainsi que la mise en application des actions correctives.

Fiche réflexe

Sécurité informatique

La sécurité informatique est un enjeu majeur lors de l'accueil de délégations étrangères. Toute connexion à un réseau interne, l'utilisation de périphériques externes non contrôlés ou l'accès à des équipements sensibles peuvent exposer l'entreprise à des risques de cyberattaques, de fuite de données ou de compromission de systèmes critiques. Il est essentiel d'adopter des mesures de protection rigoureuses, de sensibiliser les collaborateurs aux bonnes pratiques et de contrôler strictement les interactions numériques avec les visiteurs.

Contrôle des accès aux réseaux Wi-Fi

- Fournir un Wi-Fi invité distinct du réseau interne de l'entreprise.
- Restreindre l'accès aux ressources critiques (serveurs, bases de données).

Protection des postes de travail

- Désactiver les ports USB sur les ordinateurs accessibles aux visiteurs.
- S'assurer que tous les postes disposent d'un antivirus à jour.
- Appliquer des politiques de verrouillage automatique des écrans après une période d'inactivité.
- Sensibiliser les employés aux bonnes pratiques en matière de cyber sécurité.

Gestion des appareils connectés

- Interdire le branchement d'appareils personnels aux systèmes internes (ordinateurs, imprimantes, etc.).
- Ne jamais accepter une clé USB fournie par les auditeurs.
- Surveiller l'utilisation des équipements fournis temporairement aux visiteurs.
- En cas de visites très sensibles :
 - Éteindre les appareils électroniques en salle de réunion ou les laisser dans les bureaux,
 - Demander aux auditeurs de laisser leurs appareils à l'accueil. Interdire la prise de photos ou vidéos

Surveillance des échanges de données

- Privilégier des plateformes sécurisées pour le partage de documents
- Utiliser uniquement des supports fournis par l'entreprise, scanner toute clé USB avant utilisation avec un logiciel de sécurité,
- Restreindre l'envoi de documents sensibles par email, sauf après validation interne.

Fiche réflexe

Interprétariat

L'interprétariat joue un rôle clé dans la communication avec les délégations étrangères. Une mauvaise interprétation peut engendrer des malentendus ou compromettre la confidentialité des échanges.

Sélection

- Sélectionner un interprète professionnel compétent dans le domaine concerné.
- En cas de recours à un nouvel interprète, demander des informations sur l'entreprise, le CV et la fonction pour réaliser les vérifications d'usage.

Neutralité

- Veiller à ce qu'il soit neutre et ne favorise pas une partie.

Confidentialité

- Briefer l'interprète en amont sur les sujets sensibles et les attentes en matière de confidentialité.
- Faire signer un accord de confidentialité avant toute intervention pour garantir la protection des informations échangées.

Préparation

- Fournir en amont un glossaire des termes techniques et certains documents clés pour garantir une traduction précise et fluide des échanges.

Communication

- Veiller à ce que toutes les communications passent par lui y compris pour l'anglais ou l'espagnol.

Fiche réflexe

Que faire en cas d'incident ?

Signaler tout incident ou demande suspecte aux autorités compétentes (SISSE, DDISSE, service de sécurité de l'entreprise).

Pendant les échanges et la visite,

- repérer les personnes insistantes (questions, accès aux documents, aux lieux)
- Signaler tout départ ou personne non présente
- Signaler toute personne ajoutée à la dernière minute

Contacteur le CMDZS

Draafzone.est@agriculture.gouv.fr
Draafzone.ouest@agriculture.gouv.fr
Draafzone.sud@agriculture.gouv.fr
Draafzone.sudest@agriculture.gouv.fr
Draafzone.sudouest@agriculture.gouv.fr
Draafzone.paris@agriculture.gouv.fr
Draafzone.nord@agriculture.gouv.fr

Contacteur le SHFDS

l-sg-shfds@agriculture.gouv.fr

Contacteur la DGS

Votre situation vous fait craindre une potentielle ingérence étrangère :

assistance-dgsi@interieur.gouv.fr

Votre situation concerne un sujet économique : [securite-](mailto:securite-economique@interieur.gouv.fr)

[economique@interieur.gouv.fr](mailto:securite-economique@interieur.gouv.fr)

Isoler immédiatement la menace

- Restreindre l'accès aux zones sensibles,
- Couper les connexions réseau si nécessaire.
- Demander immédiatement la suppression des images prises sans autorisation

Documenter l'incident

- prendre des notes précises sur l'événement (date, heure, personnes impliquées, actions entreprises).
- établir un rapport détaillé et circonstancié de l'incident.

Prévenir les autorités compétentes

- alerter immédiatement la direction, le service de sécurité
- Saisir les autorités compétentes :
 - le correspondant local de la DGS,
 - le chef de la mission défense et sécurité de zone à la DRAAF de zone
 - le SHFDS du ministère

Analyser les impacts

- évaluer les conséquences possibles sur la sécurité de l'information et la réputation de l'entreprise.

Mettre en œuvre des mesures correctives

- renforcer les contrôles,
- sensibiliser à nouveau le personnel
- réaliser un retex à froid afin de renforcer la politique de sûreté de l'entreprise et les procédures de sécurité.

**Ministère de l'agriculture, de l'alimentation et de la
souveraineté alimentaire**

- Direction générale de l'alimentation
- Service du Haut fonctionnaire de défense et de
sécurité

France AgriMer

Juin 2025