A+ A-

Entreprises : comment protéger vos données sensibles lors de déplacements à l'étranger ?

Par Bercy Infos < https://economie.gouv.fr/entreprises/bercy-infos-qui-sommes-nous> , le 19/07/2023 - Sécurité numérique LECTURE : 5 MINUTES

Vos salariés se déplacent à l'étranger dans le cadre de leurs activités professionnelles ? Attention aux données sensibles sur leurs ordinateurs, tablettes et smartphones ! Voici nos conseils à appliquer et à relayer à vos salariés.

Qu'est-ce qu'une donnée sensible ?

Une donnée « sensible », au titre de l'article 1er de la loi relative à la protection économique des entreprises < https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000501326> , peut être identifiée comme **un document ou un renseignement d'ordre économique, commercial, industriel, financier ou technique détenu par une société**.

Au sein de chaque entreprise, **la sensibilité d'une donnée est caractérisée au regard du préjudice potentiel qui pourrait résulter de sa divulgation ou de son altération**. Le diagnostic peut être conduit sur la base d'une analyse de risques au cas par cas.

En fonction de l'organisation impactée (dommage local, global, etc.), du contexte de l'évènement et de sa durée (court, moyen ou long terme), le préjudice pourra s'apprécier en termes qualitatifs (juridique, commercial, stratégique, réputationnel, scientifique, technique, concernant des intérêts souverains, etc.) et quantitatifs (impacts financiers, et/ou en termes de perte de clients, de marchés, condamnation pénale, etc.).

En savoir plus < https://www.entreprises.gouv.fr/files/files/enjeux/securite-economique/loi-de-blocage/guide-identification

Que faire avant de partir en mission à l'étranger ?

Éviter de transporter des données superflues

Il est préférable que les appareils (ordinateurs, tablettes, smartphones, disques durs, clés USB, etc.) utilisés pendant le voyage soient des **appareils dédiés à la mission**, qui **ne contiennent pas d'autres fichiers confidentiels**.

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) préconise même de ne **rien stocker sur ces appareils** et de privilégier la récupération de fichiers chiffrés sur le lieu de mission *via* deux options :

- l'accès au réseau de l'organisme avec une liaison sécurisée (1),
- la création d'une boîte de messagerie en ligne (2) spécialement créée et dédiée au transfert de données chiffrées. Notez que les informations de cette boîte devront être supprimées après lecture.

1. *Par exemple, avec un client VPN mis en place par votre service informatique.*
2. *Paramétrez impérativement votre messagerie pour utiliser le protocole HTTPS.*

Se renseigner sur la législation locale

Il serait dommageable que les appareils emportés, listés plus haut, soient bloqués et/ou vérifiés par les autorités locales lors des contrôles aux frontières.

C'est pourquoi il est conseillé de se **renseigner sur la législation locale applicable** concernant les contrôles aux frontières du matériel informatique et sur l'importation ou l'utilisation de la cryptographie.

Vous pouvez consulter ces informations en vous rendant sur le site de l'ANSSI < https://www.ssi.gouv.fr/> . Par ailleurs, le site du ministère des Affaires étrangères < https://www.diplomatie.gouv.fr/fr> et européennes donne des recommandations générales < http://www.diplomatie.gouv.fr/fr/conseils-aux-voyageurs/> .

Sauvegarder les données emportées

En cas de perte, de vol, de casse ou de saisie de vos équipements, vos données seront **définitivement perdues**.

C'est pourquoi il est conseillé de les **sauvegarder avant le voyage**, et de les conserver dans un lieu sécurisé (3) pour les récupérer en cas de problème.

3. Un support déconnecté de tout réseau fourni par votre organisation.

Créer un mot de passe fort et chiffrer les données

Afin de bien protéger vos données sur appareil, **un mot de passe fort et sécurisé < https://www.economie.gouv.fr/particuliers/creer-mot-passe-securise> est essentiel**.

Que faire pendant la mission à l'étranger ?

Faire preuve de discrétion

Dotez vos équipements (ordinateur, tablette, téléphone) d'un **filtre de confidentialité**. Cela permet de travailler pendant un trajet sans qu'on puisse lire ou photographier vos documents par-dessus l'épaule.

Ne pas communiquer d'information confidentielle en clair par téléphone ou tout autre moyen de transmission de la voix (services de VoIP comme Skype).

Surveiller les équipements

Les appareils doivent être surveillés attentivement afin d'éviter un vol. Ne jamais les laisser dans un bureau ou dans la chambre d'hôtel (même dans un coffre).

S'il faut s'en séparer, la carte SIM doit être conservée tout comme la batterie si cela est possible. Des enveloppes inviolables et câbles antivol pour ordinateurs portables existent et constituent également une parade simple dans la plupart des situations usuelles.

Ne pas utiliser des appareils offerts

Ne pas utiliser d'appareils offerts (tablette, ordinateur, clé USB, etc.) : ils peuvent contenir des logiciels malveillants.

Pour les mêmes raisons, ne pas connecter les appareils sur des postes informatiques peu fiables. L'accès à internet dans les cybercafés, les hôtels ou les lieux publics ne garantit aucune confidentialité. La vigilance est donc de mise lors d'une connexion et le pare-feu doit rester actif.

De même, il est déconseillé de recharger les équipements dans les bornes électriques libre-service. Ce type de borne peut copier vos données.

En cas de perte ou de vol de vos équipements, informer le responsable sécurité

En cas de perte, vol ou saisie par les autorités d'un équipement, **informez immédiatement le responsable de la sécurité informatique** de votre entreprise.

De même, vous pouvez vous rapprocher du **consulat français < https://www.diplomatie.gouv.fr/fr/le-ministere-et-son-reseau/annuaires-du-ministere-de-l-europe-et-des-affaires-etrangeres/ambassades-et-consulats-francais-a-l-etranger/>** avant d'entamer toute démarche auprès des autorités locales.

Que faire après la mission à l'étranger ?

Modifier les mots de passe

Comme indiqué plus haut dans cet article, il est conseillé de changer les mots de passe avant la mission.

Il est également conseillé de les modifier lors du retour en France, car ils pourraient avoir été interceptés.

Faire analyser les équipements

Lors du retour en France, il est conseillé de confier les équipements utilisés au responsable de la sécurité informatique :

- en cas de saisie de ceux-ci (police aux frontières, accueil d'une organisation, etc.) durant le déplacement,
- si des doutes existent sur l'intégrité de l'un d'eux.

Par ailleurs, l'ANSSI conseille de ne connecter aucun appareil au réseau de l'entreprise **avant d'avoir fait ou fait faire au minimum un test anti-virus et anti logiciel-espion**.

Penser enfin à **effacer l'historique des appels et des navigations** ainsi que les données laissées en mémoire cache, cookies, mot de passe d'accès aux sites Web et fichiers temporaires.

Ces contenus peuvent aussi vous intéresser

Entreprises : quelles règles de cybersécurité appliquer ?
Sécurité de vos données : quelles sont les méthodes de piratage les plus courantes ?
Comment lutter contre les spams ?
Cinq conseils pour se prémunir contre les « rançongiciels » (ransomware)
Entreprises : faites attention aux tentatives d'escroqueries !

En savoir plus sur les bonnes pratiques pour les déplacements à l'étranger

Bonnes pratiques à l'usage des professionnels en déplacement < https://www.ssi.gouv.fr/guide/partir-en-mission-avec-son-telephone-sa-tablette-ou-son-ordinateur-portable/> *sur le site de l'ANSSI*

Partir à l'étranger avec son téléphone, sa tablette ou son ordinateur portable < https://www.ssi.gouv.fr/uploads/IMG/pdf/passeport_voyageurs_anssi.pdf?v=1690362733> [PDF ; 1,64 Mo] *sur le site de l'ANSSI*

Guide à l'usage des entreprises d'identification des données sensibles < https://www.medef.com/fr/actualites/guide-afep-medef-didentification-des-donnees-sensibles-des-entreprises> [PDF – 282 Ko] *sur le site du Medef*

Ce que dit la loi

Loi dite « de blocage » < https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000501326>

Thématiques : **Sécurité numérique**

Ce sujet vous intéresse ? Chaque jeudi avec la lettre Bercy infos Entreprises, recevez les toutes les dernières actus fiscales, comptables RH et financières… utiles à la gestion de votre activité.

Partager la page