MINISTÈRES
ÉDUCATION
JEUNESSE
SPORTS
ENSEIGNEMENT
SUPÉRIEUR
RECHERCHE
Liberté
Égalité
Fraternité

Service du haut fonctionnaire de défense et de sécurité

Service de défense et de sécurité
Bureau de la protection du secret
n°2024-142
Affaire suivie par :
Jean-Emmanuel Réaubourg
Tél : 01 55 55 87 27
Mél :
jean-emmanuel.reaubourg@education.gouv.fr
99, rue de Grenelle
75007 Paris SP 07

Paris, le 08 JAN. 2024

Le haut fonctionnaire de défense et de sécurité

à

Destinataires in fine

Objet : Recommandations relatives à la protection des données professionnelles lors des déplacements à l'étranger

Références :
- Arrêté du du 09/08/202 portant approbation de l'instruction générale interministérielle sur la protection du secret de la défense nationale
- Circulaire du Premier Ministre du 26 mars 2015 sur la sécurité des agents et des implantations de la France à l'étranger[1]
-

Lors de leurs déplacements professionnels à l'étranger, les agents publics doivent respecter des mesures de protection des données professionnelles. Elles sont rappelées dans cette note qui concerne les agents des administrations centrales et des établissements exerçant une mission de service public relevant du périmètre d'attribution des ministères en charge de l'éducation nationale, de la jeunesse, de l'enseignement supérieur et de la recherche, du sport et des jeux olympiques et paralympiques.

Les présentes prescriptions et recommandations sont fondées sur des cas constatés, y compris dans le périmètre de nos ministères. Il convient donc d'y sensibiliser les personnels placés sous votre responsabilité.

1- Obligation des agents et champ des informations concernées

L'agent public « *est tenu au secret professionnel* » (code général de la fonction publique, article L. 121-6°). Il « *doit faire preuve de discrétion professionnelle pour tous les faits, informations ou documents dont il a connaissance dans l'exercice ou à l'occasion de l'exercice de ses fonctions* » (article L. 121-7).

Cette obligation impose à l'agent de veiller à la non-divulgation d'informations obtenues dans le

[1] http://circulaire.legifrance.gouv.fr/pdf/2015/03/cir_39401.pdf

cadre de l'exercice professionnel. Cette prescription concerne particulièrement les informations qui peuvent revêtir un caractère sensible et dont la divulgation pourrait nuire aux intérêts publics.

« *Sont considérées comme sensibles :*
- les informations couvertes par le secret des délibérations du Gouvernement ;
- les données à caractère personnel ;
- plus largement, les informations stratégiques et organisationnelles, les informations techniques et technico-commerciales, les informations commerciales et les données économiques et financières.
- les données de recherche entrant dans le champ de la protection du potentiel scientifique et technique. » (code des relations entre le public et l'administration, article L. 311-5).

Tout manquement à cette obligation peut donner lieu à des sanctions administratives et disciplinaires.

La vigilance en matière de protection de ces documents et informations s'impose dans le cadre général de l'exercice professionnel, de missions en particulier à l'étranger, dans des zones sensibles ou non. Elle s'attache tant aux supports physiques que numériques.

2- Recommandations lors des déplacements professionnels :

a) Démarches préalables au déplacement :

Selon la nature du pays et les missions, les agents veilleront à :

- Consulter le site du MEAE (page « Conseils aux voyageurs » et s'inscrire sur le portail ARIANE si le déplacement se confirme[2]), cette consultation n'est pas obligatoire mais fortement recommandée ;

- S'assurer que le pays en question ne présente pas de risques géopolitiques, d'impact ou de vulnérabilités au regard des missions exercées par l'agent.

Les recommandations qui suivent sont extraites en grande partie du « Passeport de conseils aux voyageurs » de l'ANSSI, qu'il est fortement conseillé de consulter avant tout départ[3].

Recommandations :

b) Avant le départ et pendant les trajets :

- Minimiser le nombre d'équipements numériques transportés ;
- Changer les mots de passe de messagerie et d'ouverture de session d'ordinateur avant et après le voyage ;
- Éviter de partir avec des données sensibles en déplacement ; privilégier la récupération et le stockage de ces données depuis un espace sécurisé en ligne (filesender.renater.fr par exemple) ;
- Sauvegarder les données emportées et laisser la sauvegarde en lieu sûr ;
- Apposer un filtre de protection d'écran d'ordinateur, afin de travailler pendant les trajets sans que des tiers puissent lire ou photographier les documents ;
- Marquer ses appareils d'un signe distinctif (ex.: pastille de couleur), afin de mieux surveiller le matériel et de s'assurer qu'il n'y a pas eu d'échange, notamment pendant le transport ;

2 France Diplomatie – Conseils aux voyageurs : https://www.diplomatie.gouv.fr/fr/conseils-aux-voyageurs/

3 ANSSI - Passeport de conseils aux voyageurs : https://www.ssi.gouv.fr/uploads/IMG/pdf/passeport_voyageurs_anssi.pdf

Pour les déplacements dans un pays sensible :

Ne pas partir avec son matériel bureautique habituel, mais utiliser un poste banalisé[4] ne contenant que des données non sensibles nécessaires à la mission.

Cette recommandation concerne surtout les agents détenant des données sensibles, c'est-à-dire, entre autres, et en application des dispositions de l'article L. 311-5 du code des relations entre le public et l'administration citées plus haut, les données :

- Personnelles ;
- Relatives aux systèmes d'information ;
- Aux marchés publics ;
- Aux recherches menées au sein de laboratoires protégées par une zone à régime restrictif (ZRR) au titre de la protection du potentiel scientifique et technique (PPST) ou menées avec des industriels ou dans les domaines de la défense, de l'espace, du nucléaire, du quantique, de l'intelligence artificielle ou liées à des secteurs économiques stratégiques.

Cette liste n'est pas exhaustive. En cas de doute, il convient d'interroger, dans les établissements d'enseignement supérieur et de recherche, le fonctionnaire de sécurité de défense (FSD) et, dans les services de l'éducation nationale, de la jeunesse et des sports, le correspondant PSDN du rectorat et les responsables de la sécurité des systèmes d'information (RSSI) pour les données numériques. Dans tous les cas, le service de défense et de sécurité ministériel (bureau de la protection du secret) peut également apporter son expertise.

c) Pendant le séjour :

- Garder les appareils, supports, fichiers et documents au plus près de soi (y compris la nuit) :
  - Ne jamais les laisser hors de surveillance dans les lieux publics (salons et séminaires inclus) ;
  - Ne les laisser ni dans un bureau ni dans une chambre d'hôtel, ni à l'aéroport ou ailleurs sans surveillance (en particulier, voyager avec les équipements numériques en cabine) ;
  - Fermer fenêtres et portes du lieu où ils sont entreposés avec une mise sous clé recommandée ;
- Protéger l'accès aux appareils par des mots de passe[5] et des modalités de verrouillage fortes[6] ;
- Ne pas faire confiance aux réseaux non maîtrisés (bornes wifi publiques) pour connecter les équipements, à moins d'utiliser un VPN fourni à titre professionnel ;
- Eteindre son matériel lorsque l'on ne l'utilise pas pendant une longue période[7] ;
- Faire preuve de vigilance lors de ses conversations téléphoniques ou en visio-conférence ;
- Eviter de prendre son smartphone pendant une réunion sensible (risque de captation des échanges) ;
- Veiller aux sollicitations (propositions de partenariats, invitations festives) ; évaluer la pertinence d'une question et la réponse à apporter (besoin d'en connaître de son interlocuteur) ;

4 Un ordinateur de prêt préparé par votre service informatique et ne disposant pas de vos données locales habituelles

5 Au minimum 12 caractères comprenant chiffres, majuscules, minuscules et caractères spéciaux

6 Pour les téléphones mobiles : verrouillage biométrique (détection de visage ou d'empreintes) ou un PIN de 6 chiffres minimum

7 Les mots de passe et secrets sont stockés en mémoire dans un ordinateur en veille et sont plus facilement récupérables que dans un ordinateur éteint.

- En cas d'inspection ou de saisie du matériel par les autorités, informer immédiatement sa hiérarchie et le haut fonctionnaire de défense et de sécurité (HFDS) si des informations sensibles sont concernées ;
- Fournir les mots de passe et clés de chiffrement seulement si on y est contraint par les autorités locales ; dans ce cas, prévenir dès que possible le responsable de la sécurité des SI et le service informatique de sa structure de rattachement.

d) Au retour de la mission :

- Ne pas utiliser les équipements qui ont été offerts (clés USB). Ils peuvent contenir des logiciels malveillants. Les clés USB, du fait de leurs multiples vulnérabilités, sont un vecteur d'infection privilégié;
- Changer tous les mots de passe utilisés pendant le voyage, car ils peuvent avoir été interceptés ;
- En cas de doute, faire analyser ses équipements par les services informatiques de l'établissement ou par le RSSI selon les organisations ;
- Ne pas reconnecter les appareils au réseau informatique habituel avant d'avoir fait ou fait faire au minimum un test anti-virus par les services informatiques de l'établissement ou le RSSI ;

En cas de perte ou de vol d'un équipement ou d'informations sensibles, informer immédiatement sa hiérarchie et la chaine d'alerte (FSD/HFDS, RSSI).

Je vous remercie de veiller à la stricte application de ces mesures et de signaler, par le biais des correspondants PSDN académiques et des FSD en université, au service du haut fonctionnaire de défense et de sécurité toute difficulté dans leur mise en œuvre.

Thierry LE GOFF

Liste des destinataires

Mesdames et Messieurs les recteurs de région académique ;
Mesdames et Messieurs les recteurs d'académie ;
Mesdames et Messieurs les recteurs délégués à l'enseignement supérieur à la recherche et l'innovation ;
Madame et Messieurs les vice-recteurs ;

Mesdames les directrices générales ;
Messieurs les directeurs généraux ;

Madame la cheffe du service de l'inspection générale de l'éducation, du sport et de la recherche ;

Mesdames les directrices ;
Messieurs les directeurs ;

Mesdames les déléguées ;

Madame la cheffe du service de l'action administrative et des moyens ;

Mesdames et Messieurs les présidents ou directeurs d'établissements d'enseignement supérieur ;

Mesdames et Messieurs les directeurs des établissements publics de l'éducation nationale et de l'enseignement supérieur, de la recherche et de l'innovation ;

Mesdames et Messieurs les présidents ou directeurs d'organismes de recherche ;

Mesdames et Messieurs les présidents ou directeurs d'organismes ;

Madame la médiatrice de l'éducation nationale et de l'enseignement supérieur ;

Monsieur le président par intérim du CNOUS ;

Mesdames et messieurs les directeurs des CROUS ;

Mesdames et Messieurs les directeurs régionaux de la jeunesse, à l'engagement et aux sports.