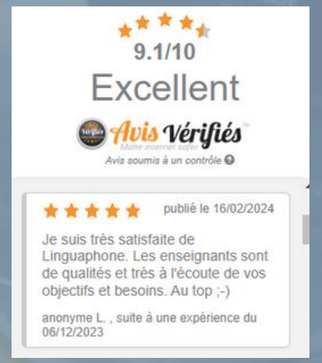
RGPD

Les bonnes pratiques

LINGUAPHONE
- 1901 -

Votre partenaire Langue
Votre partenaire de confiance



LES 5 RÈGLES D'OR DES COLLABORATEURS

1 - INFORMATION

Chaque collaborateur doit connaître la RGPD, ses enjeux et doit être capable d'identifier une donnée personnelle

2 - CONFIDENTIALITE

Chaque collaborateur doit observer une stricte confidentialité concernant les données personnelles

3 - SECURITE INFORMATIQUE

Chaque collaborateur doit respecter toutes les pratiques prévues par notre société en termes de sécurité informatique

4 - ESPACE DE TRAVAIL

Chaque collaborateur veille à protéger les données personnelles et à ne les partager que dans un cadre précis

5 - VIGILANCE ET PROCESS RGPD

Faire remonter à votre chargé de mise en œuvre qui se chargera de contacter le DPO en cas d'incidents (violation de données) ; de risque potentiel ; de doutes ; ...

Bonnes pratiques informatiques

Utiliser un mot de passe complexe (Minuscules, majuscules, chiffres, caractères spéciaux)
Ne pas utiliser les mêmes mots de passe pour la session et pour les applicatifs
Ne pas utiliser le même mot de passe pour ses activités professionnelles et personnelles
Ne jamais communiquer son mot de passe à autrui
Ne pas stocker son mot de passe sur un navigateur : préférer un logiciel comme « LastPass »
Ne pas sauvegarder ses mots de passe sur un fichier (word ou autre) ou les noter sur un support physique (cahiers, post-it…)

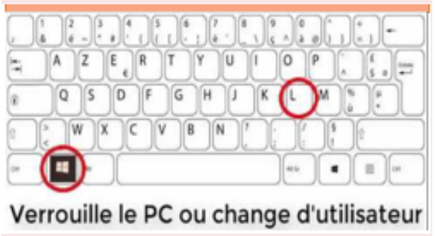
Ne consulter une pièce jointe que si l'émetteur est de confiance et le contenu du mail cohérent
Ne pas ouvrir les fichiers dont les extensions sont : .VBS ; .JBS ; .SHS ; .PIF ; .EXE ; .BAT ou .COM
Ne pas répondre aux mails demandant des informations personnelles
Ne pas saisir son mot de passe via un lien vous demandant de vous authentifier : préférer aller sur le site de l'éditeur
Ne pas se connecter à sa messagerie professionnelle via un appareil personnel
Ne pas faire suivre un mail professionnel sur sa messagerie personnelle

Ne pas utiliser de support amovible personnel (clef USB, disque dur externe…)
Ne pas stocker de données professionnelles sur ses appareil personnels

Appliquer les mises à jour prévues par le système le plus rapidement possible (éviter de les reporter)

Télécharger uniquement des logiciels professionnels et uniquement depuis les sites officiels)

Verrouiller son écran dès que l'on s'absente de son poste de travail (y compris en télétravail), même pour quelques instants



Limiter ses recherches personnelles à des sites fiables et reconnus

Penser à sauvegarder régulièrement ses travaux

Eviter de se connecter sur des réseaux wi-fi partagés (publics)
En dehors des locaux : se connecter au VPN

Bonnes pratiques informatiques

Avertir immédiatement son responsable qui alertera le DPO dès lors qu'une **violation de données** est constatée

Informer le DPO via son responsable dès lors qu'une **évolution de procédure/un nouvel outil** est susceptible d'entrainer : la collecte de nouvelles données ; l'accès à plus de données ; un risque de violation de données

Veiller au respect des droits des personnes

Ne pas renseigner un tiers sauf exceptions prévues dans les procédures internes
Ne pas enregistrer d'informations pour un mineur de moins de 15 ans sans le consentement des représentants légaux. **Demander la suppression** de la fiche !
Attention aux espaces mémos : ne renseigner que les informations absolument nécessaires et jamais de données sensibles ou hautement personnelles
Ne pas collecter directement les coordonnées bancaires (numéro de CB). Ne jamais les noter. Indiquer au client la marche à suivre pour les saisir lui-même.
Ne pas utiliser de courriers ou mails nominatifs comme modèle. Préférer un modèle anonyme.
Vérifier le nom, prénom et adresse du destinataire avant envoi.

Limiter les échanges de fichier par mail au maximum (protéger les pièces jointes sensibles par un mot de passe)
Protéger les fichiers communs par un mot de passe donné uniquement aux utilisateurs légitimes
Supprimer ou anonymiser tout fichier dès qu'il n'est plus nécessaire ou qu'il est nécessaire uniquement à des fins statistiques *nb. Un numéro client/coupon est une donnée personnelle à « anonymiser »*
N'enregistrer ses fichiers que sur les espaces prévues. Les fichiers enregistrés sur son bureau ou dans sa base « téléchargement » doivent être supprimés dès que le fichier a été stocké ailleurs.
Ne pas stocker de copie de justificatif d'identité sans l'avoir rendu inutilisable (exemple : le tamponner avant enregistrement)

Fermer les armoires à clef

Ne pas laisser trainer de documents / pochettes sur les bureau

Détruire les documents physiques avant de les jeter dans une corbeille (déchiqueteuse)