RGPD : FICHE REFLEXE
Bonnes pratiques pour la protection des données

- Garder à l'esprit de **devoir agir pour la protection des individus** dont on détient des données à caractère personnel.
- Respecter **l'obligation de confidentialité** des informations professionnelles dont vous avez connaissance dans le cadre de votre service (maintenance, administrateur, …).
- **La sécurité n'est pas que technique**, elle passe également par l'utilisation que vous faites des outils mis à votre disposition.

① PROTECTION PHYSIQUE

⇨ Les locaux

✓ Etre vigilant sur l'accès aux locaux (entrées, sorties) => filtrage des allées et venues par un accueil.

✓ Pour l'accueil des usagers, délimitez une zone de discrétion (marquage au sol, borne) garantissant la sécurité des données personnelles et du secret professionnel.

⇨ L'espace de travail

✓ Maintenir un espace de travail dans lequel ne sont pas laissés, à la portée de tous (visiteurs, collègues, intervenants, équipe d'entretien, …), des dossiers contenant des données à caractère personnel. Cela concerne :

- l'ordinateur pour lequel l'accès doit être individualisé par un mot de passe personnalisé et qui doit se verrouiller après un temps d'absence relativement court.
- le bureau sur et dans lequel figurent des dossiers papier et/ou numérique (clé USB, CD, …).

⇨ La conservation

✓ Ranger les documents dans des lieux sécurisés :

- Pour l'ordinateur : arborescence numérique dont les données sont sauvegardées.
- Pour le papier et outils mobiles : armoires et portes fermées à clé, coffre, ….

✓ Détruire règlementairement les documents, avec un broyeur, lorsqu'ils contiennent des données à caractère personnel qui n'ont plus matière à exister => éviter l'utilisation des poubelles où les documents sont susceptibles d'être récupérés.

② PROTECTION INFORMATIQUE

⇨ Mot de passe

Les mots de passe sont les premiers codes d'authentification permettant l'accès à vos données personnelles et/ou professionnelles. Ils ouvrent l'accès à vos messageries, réseaux, outils de gestion, … De ce fait, ils doivent être difficilement accessibles par un tiers.

✓ Choisir des mots de passe complexes comprenant au moins 8 caractères alphanumériques (majuscules, minuscules, chiffres et caractères spéciaux). Toutefois, il est fortement recommandé de ne pas mettre votre date d'anniversaire, votre nom, prénom ou encore une suite de chiffre comme 1,2,3,4.

✓ Eviter d'utiliser le même mot de passe professionnel et personnel, afin de réduire le risque de violation de données.

✓ Les changer régulièrement par trimestre ou semestre par exemple ;

✓ Ne pas les communiquer.

✓ Mettre en place un verrouillage automatique du PC après une durée limitée d'inactivité.

⇨ Utilisation internet

- ✓ N'accéder si possible qu'à des sites sécurisés : http**s**//… ;
- ✓ Limiter la consultation de sites dans un but purement personnel ;
- ✓ Télécharger vos applications uniquement sur les sites officiels ;
- ✓ S'assurer des droits avant toute réutilisation : droit d'auteur, de propriété, d'image, plagiat…

⇨ Equipement mobile (portables, tablettes, téléphones, …) et support amovible (disques durs, clé usb, carte mémoire …)

- ✓ Ne pas les laisser à la portée de tous ;
- ✓ Les protéger avec un verrouillage (code d'accès).
- ✓ Les supports externes (clé USB, etc.) peuvent être infectés et compromettre le bon fonctionnement de votre poste de travail. Ils sont vecteurs de nombreux piratages.
  - Ne les utiliser que s'ils proviennent d'une source sûre.

⇨ Outils de protection

- ✓ Activer le pare feu ;
- ✓ Utiliser un antivirus ET veiller à sa mise à jour régulière ;
- ✓ Ne pas désactiver les paramétrages de sécurité.

⇨ Sauvegarde

- ✓ Sauvegarder régulièrement vos documents ;
- ✓ Les stocker sur les espaces réservés à cet effet (serveur, disque dur externe, etc.).
- ✓ Appliquer les mises à jour de sécurité sur tous vos appareils et ce, dès qu'elles vous sont proposées

En cas de sauvegarde via un outil externe (disque dur externe), sécuriser le lieu d'accès à celui-ci pour le protéger du vol et permettre la récupération de vos données. Concernant les outils de sauvegarde virtuel (cloud), vérifier la conformité du prestataire.

③ PROTECTION DES COMMUNICATIONS

- ✓ Préserver la vie privée des usagers, en les informant de leurs droits et en évitant de leur poser des questions présentant des données à caractère personnel dans les espaces communs/publics où d'autres personnes peuvent être présentes (accueil dans un bureau individuel).

- ✓ Si possible, ne pas communiquer les coordonnées professionnelles personnalisées des agents (nom, prénom, adresse mail) mais privilégier les références service.

⇨ Utilisation de la messagerie :

- ✓ En tant que destinataire : méfiez-vous des messages inattendus.
  - ✓ Identifier les expéditeurs avant d'ouvrir les messages ; demandez toujours confirmation à l'émetteur par un autre moyen si il vous semble connu et légitime (mesure de protection contre l'hameçonnage)
  - ✓ Vérifier les liens des corps de message et les pièces jointes avant de les ouvrir (xxx.exe) ;
  - ✓ Ne pas utiliser d'adresse personnelle ;
  - ✓ Signaler un courrier indésirable à votre support technique ou à votre hiérarchie.
- ✓ En tant qu'expéditeur :
  - ✓ N'envoyez aucune donnée sensible par courriel.

Rappel de l'Article 226-22 du Code Pénal :

"Le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

La divulgation prévue à l'alinéa précédent est punie de trois ans d'emprisonnement et de 100 000 euros d'amende lorsqu'elle a été commise par imprudence ou négligence.

Dans les cas prévus aux deux alinéas précédents, la poursuite ne peut être exercée que sur plainte de la victime, de son représentant légal ou de ses ayants droit."

Plus d'informations

Délégué à la protection des données
Rue François Arago – 61250 Valframbert
06.21.77.92.58
rgpd@cdg61.fr
www.cdg61.fr