RGPD
Quelques pistes de gestion des mails

CONTEXTE

Une enquête révèle qu'en 2020, 88 courriels sont reçus et 34 sont envoyés en moyenne par jour, par entreprise et par salarié. Ce chiffre a doublé en moins d'une dizaine d'années.

Hormis les incidences néfastes sur les conditions de travail que ce nouveau mode de gestion du travail peut induire, il génère également des risques en matière de protection de la vie privée des personnes concernées par l'échange.

Cette fiche a pour but de recenser quelques bonnes pratiques afin d'améliorer et d'optimiser l'utilisation de la messagerie de manière efficace et sécurisée.

COMMENT PROCEDER ?

S'approprier l'outil avec l'appui de mesures organisationnelles et techniques.

Il s'agira d'inscrire une politique de gestion commune, partagée de tous, en sus de la charte informatique, qui définisse la gestion et les outils de la messagerie pour sécuriser les échanges et éviter l'éventuel sentiment de surcharge, de perte de temps de traitement, ….

Quelques pistes

- **De sécurité :**

❖ Utiliser des agenda et carnet d'adresses partagés => Déclarer la base adresses au registre des traitements de données personnelles

❖ Respecter une charte graphique => Prévoir un même nom de domaine pour toutes les adresses du type : *service@nomcollectivité.fr* (pas de nom de personne) ; Prévoir un bandeau de signature avec logo. A défaut de sécurisation des mails, qui reste à privilégier, prévoir un message de sécurité en bas des mails sortants dit « disclaimer ».

❖ Identifier le mode de fonctionnement le plus approprié pour l'activité =>

. En cas de messagerie centralisée :

- Qui doit traiter un mail en particulier ? Définir qui lit le courrier, le traite ou le transmet. Exemple, agent d'accueil ou direction générale ?
- Dans quel cas répondre directement, dans quel cas transférer à son responsable ?
- Comment s'assurer qu'une réponse a bien été apportée (et ne pas répondre deux fois au même message...) ?
- Comment vérifier ce qu'a répondu un collègue, en son absence ?
- Ne pas surcharger ses destinataires : une seule personne destinataire, seules les personnes indispensables en copie ; Éviter les copies cachées, sauf en cas de données personnelles à protéger ; Limiter la fonction « Répondre à tous » ; Limiter les accusés-réception ; Plutôt que des pièces-jointes, préférer des liens vers des documents en ligne ou un chemin vers un répertoire partagé.

. Idem <u>en cas de messagerie « en libre-service »</u> (utilisateur qui traite directement les messages le concernant) :

- Définir les circuits : quelle personne, ou quel service, a la responsabilité de répondre à quelles natures de demandes - Définir les niveaux d'habilitation : habilitation d'une personne à répondre directement ou nécessité d'en référer à son responsable ?
- Harmoniser les modes de réponse : Sous quel délai sont traitées certaines demandes ? Faire un mail d'accusé-réception ? prévoir le délai dans celui-ci ? Préparer des réponses-types à certaines questions récurrentes.

❖ Gérer les redirections de messages => définir des règles, temps de conservation, fin de redirection (cessation de fonctions, …).

❖ Utiliser d'autres outils collaboratifs : (groupware, intranet, applications métier).

❖ Organiser sa boite de réception => par exemple, ne laisser dans la boîte de réception que les mails non traités.

❖ Appliquer une action à la lecture de chaque mail => Traiter, tagguer, supprimer ou transférer, ranger.

❖ Créer une arborescence par thématiques, durée de validité de messages, … afin de faciliter la recherche d'information difficiles.

❖ Nettoyer sa messagerie à échéance régulière en classant ses mails dans les dossiers correspondants, en les archivant ou en stockant les pièces-jointes et les mails sur le réseau => Mettre une arborescence adéquate sur serveur.

❖ Paramétrer un classement automatique, mettre des signets, …

❖ Prévoir une politique d'archivage (conservation/destruction) des mails.

❖ Se désabonner des newsletters qui n'ont plus d'utilité.

❖ Communiquer sur sa politique en interne et en externe.

❖ Informer sur les risques de piratages, les protection, sécurité et conformité => Développer la vigilance des utilisateurs pour reconnaître et gérer :

- les **virus** : logiciel qui s'installe après ouverture d'une pièce jointe contaminée soit, avoir un antivirus à jour. Vérifier la source de la réception.
- les **hoax** : rumeurs véhiculées par mails => Éviter de transférer les hoax,
- l'**hameçonnage** : mail visant à récupérer des informations personnelles de la victime => Vérifier la source, Éviter de transmettre des informations personnelles par mails.
- le **spam** : mail anonyme envoyé en masse à des fins commerciale ou malhonnête => Éviter de répondre ou de transférer le message.

❖ Gérer les messages contenant de la donnée sensible (santé, RH, Paie, …) => solution de cryptage (chiffrement) des mails afin de sécuriser les échanges.

- **D'efficacité :**

❖ Veiller à la qualité de rédaction du contenu : pas de mail trop familier, de texte dense ou peu compréhensible. En cas de doute, vérifier l'identité de l'émetteur => Le message doit être bien structuré : objet, formule d'appel, introduction, développement, conclusion. Appliquer les règles de courtoisie avec des formules d'appel et de politesse. Préciser également l'objet, ce dernier permettra l'information et, le cas échéant, facilitera la recherche.

❖ Regrouper les temps de consultation des mails en supprimant les alertes sonores ; s'astreindre à éteindre son téléphone pendant les réunions ; veiller à ne pas envoyer de mails en dehors des heures habituelles de travail.

❖ Éviter la communication par mail dans les situations suivantes :
- Conflit ou émotion « mail à chaud »
- Echanges sans fin où la réunion est préférable
- Difficulté à gérer engendrant un renvoi ou l'évitement

A SAVOIR

Les messages envoyés ou reçus depuis le poste de travail sont à priori à caractère professionnel, sauf à ce que leur contenu intéresse la vie privée de l'auteur en matière de santé, patrimoine, affective ou sexuelle.

Les messages personnels doivent être identifiés en tant que tel : - Exemple : par la mention dans l'objet « personnel » ou « privé » ; Ils sont alors protégés par le secret des correspondances (jurisprudence Nikon)

Le contrôle de l'employeur reste possible avec mesure :

- Possibilité de mettre en œuvre des moyens techniques de contrôle (outils de mesure de fréquence des messages envoyés ou reçus, de la taille des fichiers, des outils d'archivage des messages échangés).
- L'information de l'agent relative au contrôle, via la charte informatique, par exemple, est obligatoire. Également pour la durée de conservation des messages.
- La présence de l'agent en cas de consultation est obligatoire. En cas de dérogations, celles-ci doivent être connues de l'intéressé.
- Le contrôle ne doit pas être motivé pas le seul objectif de surveillance des agents ; il doit avoir un intérêt légitime et être animé par des motifs strictement professionnels.

LES DURÉES DE CONSERVATION

- Mails et dossiers de classement : En général, 6 mois avant archivage puis destruction au bout d'un an ; Les messages devant être conservés doivent l'être par intégration des éléments dans le dossier adéquat hors messagerie (sur serveur).
- Fichiers journaux : 3 mois glissants maximum
- Logs de connexion : 1 semaine
- Contacts : sur la durée d'existence du lien d'échange => mise à jour à réaliser régulièrement.
- Définir la durée de conservation des données issues des comptes de messagerie des agents => par exemple, 1 mois après le départ de l'agent.

CADRE JURIDIQUE

- Loi sur les droits et obligations des fonctionnaires 83-583 du 13 juillet 1983 Art. 26, 29.
- Loi « Informatique et libertés » du 6 janvier 1978
- Code Civil – Art. 9 « *Chacun a droit au respect de sa vie privée. /…* »
- CAA de Rennes, 14.01.2010 : L'usage de la messagerie professionnelle est en principe réservé à une finalité professionnelle.

EN SAVOIR PLUS

- Appui sur les Charte informatique et bonnes pratiques
- CNIL : lien vers comment chiffrer documents et répertoires et sa préconisation de tolérance de l'usage personnel de la messagerie professionnelle dans la limite du raisonnable.