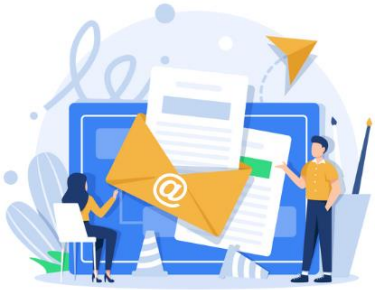
Focus sur la messagerie professionnelle au travail

La messagerie professionnelle est aujourd'hui devenue un outil indispensable pour l'accomplissement, par l'employé, de ses missions de travail.

Toutefois, la banalisation d'un tel dispositif de communication électronique n'exonère pas pour autant l'employeur du respect des dispositions relatives à la protection des données personnelles, et bien qu'il puisse, dans certains cas, décider de procéder au contrôle ou à la surveillance de l'utilisation de la messagerie mise à disposition de ses salariés, notamment pour des raisons de sécurité, il est tenu également par l'obligation de respecter la vie privée de ces derniers.



Quid du respect de la vie privée des salariés

En Principauté, conformément à l'article 22 de la Constitution, « *Toute personne a droit au respect de sa vie privée et familiale et au secret de sa correspondance* ».

De même, dans un arrêt *Niemietz c. Allemagne* en date du 16 décembre 1992, la Cour Européenne des Droits de l'Homme (CEDH) a consacré le droit au respect de la vie privée sur le lieu de travail en se fondant sur l'article 8 de la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales, aux termes duquel *« Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance ».*

Quelques années plus tard, cette même Cour a précisé les conditions dans lesquelles l'employeur peut consulter les communications numériques de son salarié dans son arrêt *Bărbulescu c. Roumanie* en date de 2017.

En l'espèce, un salarié qui avait communiqué avec sa famille à partir de son poste de travail, sur un compte de messagerie destiné à un usage professionnel, avait été licencié, au motif qu'il n'avait pas respecté le règlement intérieur qui interdisait l'utilisation des ressources de l'entreprise à des fins personnelles.

La Cour a toutefois estimé que ce licenciement était contraire au droit à la protection de la vie privée, consacré à l'article 8 de la Convention puisque si l'employeur est en droit de surveiller les communications électroniques de son salarié, l'étendue de la surveillance et le degré d'intrusion dans la vie privée du salarié ne doivent pas être disproportionnés par rapport au but recherché.

Par ailleurs, il incombe aux juges de vérifier que l'accès au contenu des communications n'a été mis en place que parce qu'il n'existait pas de mesures moins intrusives, et de s'assurer que les conséquences de la surveillance pour le salarié ne sont pas disproportionnées par rapport au but recherché.

Dans quels buts un employeur peut-il mettre en place une messagerie professionnelle ?

Les données personnelles peuvent être collectées pour **plusieurs finalités**, à condition que ces finalités soient :

- **déterminées** ;
- **explicites** ;
- **légitimes** ; et
- **non traitées ultérieurement de manière incompatible** avec ces finalités.

En vertu de ce principe de **limitation des finalités**, l'APDP considère que la mise en place d'une messagerie professionnelle peut répondre aux objectifs suivants :

- l'échange de messages électroniques en interne ou avec l'extérieur ;
- l'historisation des messages électroniques entrants et sortants ;
- la gestion des contacts de la messagerie électronique ;
- la gestion des dossiers de la messagerie et des messages archivés ;
- l'établissement et la lecture de fichiers journaux ;
- la gestion des habilitations d'accès à la messagerie ;
- la gestion de l'agenda ;
- l'établissement de preuves en cas de litige avec un client/employé (en cas de contestation d'un ordre, etc..).

Par ailleurs, lorsqu'une surveillance est mise en œuvre sur le lieu de travail, la messagerie professionnelle peut également avoir pour objectif(s) :

- la mise en place d'une procédure de contrôle gradué ;
- le contrôle au moyen d'un logiciel d'analyse des messages électroniques entrants ou sortants.

Quid de la notion de surveillance ou de contrôle
Un employeur peut décider de procéder au contrôle ou à la surveillance de l'utilisation de la messagerie professionnelle mise à la disposition de ses employés. A cet égard, l'APDP considère que cette notion de contrôle ou de surveillance de la messagerie électronique se conçoit comme « *toute activité qui, opérée au moyen d'un logiciel d'analyse du contenu des messages électroniques entrants et/ou sortants, consiste en l'observation, la collecte ou l'enregistrement, de manière non occasionnelle, des données à caractère personnel d'une ou de plusieurs personnes, relatives à des mouvements, des communications ou à l'utilisation de la messagerie électronique* ».

Quelle justification pour la mise en place d'une messagerie professionnelle ?

Pour être licite, un traitement automatisé de données personnelles doit répondre à au moins une des exigences prévues à l'article 5 de la Loi n° 1.565 du 3 décembre 2024.

L'APDP estime ainsi que la mise en place d'une messagerie professionnelle peut être justifiée par :

- ***Le respect des obligations légales du responsable du traitement***

Certains responsables du traitement sont soumis à des obligations particulières de **vigilance** ainsi que de **traçabilité des opérations effectuées**. Ainsi, pour les établissements bancaires ou assimilés, de telles obligations sont prévues, entre autres, par les textes suivants :

- la Loi n° 1.338 du 7 septembre 2007 sur les activités financières et son Ordonnance Souveraine d'application ;
- la Loi n° 1.362 du 3 août 2009 relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption, et son Ordonnance Souveraine d'application ;
- la Loi n° 1.314 du 29 juin 2006 relative à l'exercice d'une activité de conservation ou administration d'instruments financiers ;
- l'Arrêté Ministériel n° 2012-199 du 5 avril 2012 relatif aux obligations professionnelles des établissements de crédit teneurs de comptes-conservateurs d'instruments financiers.

Afin de respecter ces obligations, l'APDP estime que les responsables du traitement ou leurs représentants peuvent mettre en place des procédures de surveillance ou de contrôle des messageries électroniques, dans le strict respect toutefois des principes définis par la Loi n° 1.565 du 3 décembre 2024, notamment les principes de **proportionnalité** et de **transparence**

- ***La réalisation d'un intérêt légitime poursuivi par le responsable de traitement ou un tiers***

L'APDP considère qu'une procédure de surveillance ou de contrôle des messageries électroniques peut également être justifiée par un **intérêt légitime** du responsable du traitement ou d'un tiers, tel que :

- l'optimisation de l'accomplissement des missions de travail de ses employés ;
- la sécurité et le bon fonctionnement technique du réseau ou système informatique ;
- le contrôle du respect des règles internes d'usage des outils de communication électronique, du règlement intérieur, (…) ;
- la préservation des intérêts économiques, commerciaux ou financiers du responsable de traitement ou de son représentant ;
- la protection contre tout acte susceptible d'engager sa responsabilité civile ou pénale, ou de lui porter préjudice ;
- la prévention de faits illicites.

Cette dernière justification est la plus utilisée par les responsables du traitement. Ceux-ci doivent néanmoins trouver le **juste équilibre** entre des intérêts apparemment contradictoires, mais néanmoins conciliables, à savoir d'un côté leurs prérogatives en tant qu'employeur et d'un autre côté le droit au respect de la vie privée et au secret des correspondances des employés.

Eu égard à l'existence d'un **lien de subordination** ou d'un **lien contractuel** entre l'employeur et l'employé, le consentement de ce dernier ne peut constituer une justification à la mise en œuvre de ce type de traitement.

Quelles garanties mettre en place pour respecter la vie privée des salariés ?

Pour l'APDP, le respect du secret des correspondances privées sur le lieu de travail est un principe **intangible**. Ainsi, l'employeur ne peut accéder aux contenus des messages privés de ses employés envoyés ou reçus à partir de la messagerie professionnelle, sans que ledit employé soit présent, et en soit expressément d'accord.

Toutefois, pour que les messages soient considérés comme personnels, il convient pour les employés de les identifier comme tels, par exemple :

- en précisant dans l'objet du message des mots clés comme « ***privé*** », « ***[PRV]*** » ou encore « ***personnel*** » ;
- en incluant dans l'objet du message une mention laissant manifestement supposer que ledit message est privé, telle que « *vacances au Japon* » ;
- en stockant les messages dans un répertoire intitulé « *personnel* » ou « *privé* ».

L'APDP considère donc comme excessive la pratique consistant pour l'employeur à recevoir tous les messages envoyés ou reçus par ses employés puisque cette pratique ne permet pas de distinguer entre les messages professionnels et personnels desdits employés.

Par ailleurs, seule une autorisation du juge peut permettre à l'employeur d'accéder licitement aux messages privés de ses employés lorsque ces derniers n'ont pas autorisé l'employeur à lire leurs messages privés, et cela même si l'employeur a des motifs légitimes de suspecter des actes de concurrence déloyale ou toute autre atteinte portée à ses intérêts ou à la Loi. Cela peut notamment prendre la forme d'une Ordonnance judiciaire mandatant un huissier de justice aux fins d'accéder, voire d'enregistrer les messages privés litigieux.

Quelles informations peuvent être collectées ?

Conformément aux dispositions de l'article 4 de la Loi n° 1.565 du 3 décembre 2024, les données à caractère personnel collectées doivent être « *adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles sont traitées* ».

L'APDP considère ainsi que seules les données personnelles suivantes peuvent être collectées et traitées

- Données communes à l'ensemble des messageries :

- identité : nom, prénom, identifiant ;
- messages : date, heure, information expéditeurs/destinataires, contenu, objet ;
- gestion des contacts : nom, prénom, raison sociale, (…) ;
- données d'identification électronique : adresse de messagerie électronique ;
- journalisation des accès : logs de connexion des personnels habilités à avoir accès au traitement ;
- fichiers journaux : date et heure du message, nombre de messages entrants et sortants, de messages nettoyés, de spams ; volume, format, pièces jointes, noms de domaine expéditeurs de messages, (…).

- Données particulières aux messageries mises en œuvre à des fins de surveillance ou de contrôle :

- gestion des alertes : réception des alertes automatiques en fonction des niveaux hiérarchiques concernés.

Combien de temps peuvent être conservées les données collectées et traitées par une messagerie professionnelle ?

Les données personnelles collectées **ne peuvent être conservées indéfiniment** sous une forme permettant l'identification des personnes concernées.

Ainsi, l'APDP demande à l'employeur de prévoir les durées de conservation des données suivantes :

- **S'agissant de l'administration de la messagerie électronique (identité, gestion des contacts, données d'identification électronique)** : 3 mois **maximum** après le départ définitif de l'utilisateur.

A cet égard, l'APDP rappelle que lors du départ définitif de l'utilisateur, sa boite mail nominative doit être immédiatement « ***bloquée*** » c'est à dire qu'elle ne doit plus pouvoir recevoir d'e-mails, ni en envoyer, à l'exception d'un message automatique qui sera adressé à chaque personne ayant envoyé un e-mail à l'adresse concernée.

Ce message automatique a vocation à informer l'expéditeur de l'e-mail que son interlocuteur ne travaille plus au sein de l'entité, et qu'il devra désormais envoyer ses e-mails à telle ou telle adresse. Ceci pourra être pratiqué pendant 3 mois au maximum, selon les fonctions et le degré de responsabilité de l'ancien salarié.

A l'échéance de cette période de trois mois maximum, l'adresse e-mail nominative de l'ancien salarié sera désactivée (supprimée).

L'employeur doit toutefois permettre au salarié de récupérer les e-mails privés susceptibles de se trouver dans sa boite mail nominative professionnelle.

- **S'agissant du contenu des messages émis et reçus :**

L'APDP reconnait que les messages électroniques des collaborateurs peuvent être conservés durant plusieurs années notamment en ce qui concerne les établissements bancaires et assimilés à des fins de traçabilité des opérations financières, ou en cas de soupçons d'activités illicites.

Elle demande en conséquence que les messages soient régulièrement triés et qu'une politique d'archivage soit mise en place jusqu'à ce que la conservation desdits messages ne soit plus nécessaire.

- **S'agissant des logs d'accès et des fichiers journaux** : 1 an maximum, en fonction de l'activité exercée.

- **S'agissant des alertes lorsque la messagerie est mise en place à des fins de surveillance :** l'APDP demande que celles-ci soient extraites et sécurisées (non altérables). Les données relatives à un évènement ne mettant pas en lumière un incident doivent ensuite être supprimées une fois que la vérification concluant à une absence d'incident a été effectuée.

  En cas d'incident avéré les données doivent être conservées **uniquement le temps nécessaire** à la réalisation de l'enquête associée, conformément aux procédures internes et à la législation applicable.

En tout état de cause, l'APDP recommande, lorsque cela est possible, d'adopter une durée de conservation moindre, dès lors que les données traitées ne sont plus nécessaires à la réalisation de la ou des finalité(s) pour laquelle/lesquelles elles ont été initialement collectées.

Enfin, elle rappelle que dans le cadre de l'ouverture d'une procédure contentieuse, toute information nécessaire issue du traitement pourra être conservée jusqu'à la fin de ladite procédure.

Comment informer les personnes concernées ?

- ***Modalités d'information des utilisateurs***

Tout employeur doit impérativement responsabiliser les utilisateurs à la protection de leurs données personnelles.

Dans un souci de **transparence** envers les utilisateurs, ainsi que de **loyauté** dans la collecte et le traitement des informations nominatives, l'APDP recommande donc à l'employeur de mettre en place une charte d'usage des outils de communication électronique, venant préciser, notamment :

- les modalités d'identification des messages privés ;
- la procédure d'accès à la messagerie par des personnes habilitées, en cas d'absence temporaire ou définitive de l'utilisateur, et ce afin d'assurer la continuité des activités.

- ***Modalités d'information des tiers destinataires***

L'APDP recommande l'insertion d'une mention d'information au bas de tout message électronique sortant, afin d'informer les tiers destinataires de la finalité du traitement, ainsi que de leurs droits.

Exemple de message :
[Nom de l'entité à renseigner] traite vos données à caractère personnel dans le cadre des échanges via sa messagerie électronique professionnelle. Les messages échangés sont conservés [ajouter durée(s) de conservation] *Pour exercer vos droits d'accès, de rectification et de suppression de vos données, vous pouvez envoyer un e-mail à l'adresse [e-mail à renseigner] ou un courrier postal à [adresse à renseigner].* *Pour de plus amples informations, vous pouvez consulter [Lien vers une information plus complète à ajouter]*

Qui peut avoir accès aux données issues de la messagerie professionnelle ?

L'accès aux données de la messagerie professionnelle doit être limité aux **seules personnes** qui, dans le cadre de leur fonction, peuvent **légitimement en avoir connaissance au regard des objectifs du dispositif**.

Outre les salariés qui ont tous les droits sur leur propre messagerie, d'autres services en interne peuvent selon les cas avoir également accès aux informations d'une messagerie professionnelle tels que par exemple les agents habilités par les titulaires des comptes, (par délégation), les équipes en charge des alertes ou encore les administrateurs système.

De même, un prestataire informatique peut également avoir tous les droits sur une messagerie professionnelle à des fins de maintenance.

Concernant ce dernier, l'APDP rappelle que ses droits d'accès doivent alors être limités à ce qui est **strictement nécessaire à l'exécution de son contrat de prestation de service**. De plus, ledit prestataire est soumis aux mêmes obligations de sécurité et de confidentialité que celles imposées au responsable du traitement.

Dispositions à prendre en cas d'absence de l'employé
Afin d'assurer la continuité des affaires de l'entreprise pendant l'absence d'un salarié (congés, maladie, etc.), l'APDP estime que l'employeur pourra avoir accès aux messages professionnels dudit salarié, en utilisant une des méthodes suivantes : • mise en place d'une réponse automatique d'absence du bureau à l'expéditeur avec indication des personnes à contacter en cas d'urgence ; • désignation d'un suppléant qui dispose d'un droit d'accès personnalisé à la messagerie de son collègue ; • transfert à un suppléant de tous les messages entrants. Dans les deux derniers cas, le salarié devra toutefois être informé de l'identité de son suppléant et ce suppléant ne devra pas lire les messages identifiés comme privés ou personnels.

L'APDP estime par ailleurs que la communication des données à la Direction de la Sûreté Publique peut être justifiée pour les besoins d'une enquête judiciaire.

A cet égard, elle rappelle qu'en cas de transmission, ladite Direction ne pourra avoir communication des informations que dans le strict cadre de ses missions légalement conférées.

Enfin, l'APDP considère que l'Autorité Monégasque de Sécurité Financière (AMSF) et la Commission de Contrôle des Activités Financières (CCAF) peuvent, dans le cadre exclusif des missions qui leur sont conférées, être destinataires de données personnelles traitées.

Quelle sécurité mettre en place ?

L'APDP rappelle que les mesures techniques et organisationnelles mises en place afin d'assurer la sécurité et la confidentialité du traitement au regard des risques présentés par celui-ci et de la nature des données à protéger devront être maintenues et mises à jour en tenant compte de l'état de l'art, afin de permettre de conserver le haut niveau de fiabilité attendu tout au long de la période d'exploitation du traitement.

Les mots de passe doivent être **forts et régulièrement renouvelés**.

Les **accès à distance** à la messagerie doivent être **sécurisés**.

L'employeur doit en outre régulièrement **sensibiliser les utilisateurs** à la sécurité de leur messagerie (par exemple : ne jamais ouvrir les pièces jointes provenant d'un expéditeur inconnu, ne pas cliquer sur des hyperliens dans les emails, ne pas envoyer de données sensibles ou importantes par email non sécurisé).