L'employé doit-il remettre le mot de passe de son ordinateur à l'employeur ?

Réponse courte

Non, un salarié n'est pas tenu de remettre son mot de passe personnel à l'employeur, même sur un ordinateur professionnel. Le mot de passe est une **donnée d'authentification personnelle** qui garantit la sécurité du compte et la traçabilité des actions de l'utilisateur. L'exigence de communiquer ce mot de passe violerait le principe de **confidentialité** du RGPD et les règles de surveillance des salariés de l'**article L.261-1** du Code du travail. Exiger le mot de passe reviendrait également à permettre à l'employeur d'agir sous l'identité du salarié, ce qui est interdit.

L'employeur dispose cependant de **moyens légaux alternatifs** pour accéder aux données professionnelles stockées sur l'ordinateur : compte administrateur dédié, procédure de réinitialisation par le service IT, clés de chiffrement archivées, ou accès en présence du salarié. En cas d'absence imprévue, de départ ou de litige, ces dispositifs permettent de garantir la **continuité d'activité** sans porter atteinte à la vie privée du salarié. Les fichiers et emails marqués "privé" ou "personnel" restent protégés même si l'employeur accède légitimement au poste de travail.

Définition

Le **mot de passe personnel** est une donnée d'authentification connue du seul utilisateur qui garantit l'identification unique de l'auteur d'une action informatique. Il se distingue du **mot de passe administrateur** (partagé entre les responsables IT pour des besoins de maintenance) et des **clés de chiffrement** (archivées dans un coffre numérique séparé). Au Luxembourg, la CNPD et les règles générales de cybersécurité considèrent que la communication d'un mot de passe personnel à un tiers, y compris l'employeur, affaiblit la sécurité globale du système d'information et rompt la traçabilité individuelle des actions.

Conditions d’exercice

L'accès de l'employeur aux données stockées sur l'ordinateur d'un salarié doit respecter plusieurs principes cumulatifs qui interdisent l'exigence du mot de passe personnel tout en garantissant la continuité d'activité.

Principe	Détail
Confidentialité du mot de passe	Le mot de passe personnel reste strictement confidentiel (art. 32 RGPD)
Présomption professionnelle	Les fichiers et emails sans mention privée sont présumés professionnels
Protection du privé	Les éléments marqués "privé" ou "personnel" sont protégés de l'accès
Continuité par compte admin	L'employeur dispose d'un compte administrateur technique distinct
Information préalable	Charte informatique précisant les modalités d'accès
Consultation délégation	Avis préalable sur les procédures d'accès (art. L.414-1)
Traçabilité	Journalisation de chaque accès effectué en l'absence du salarié

Modalités pratiques

Plutôt que d'exiger le mot de passe personnel, l'employeur doit mettre en place des dispositifs techniques et organisationnels qui permettent un accès légitime aux données professionnelles sans compromettre l'authentification individuelle du salarié.

Dispositif	Détail
Compte administrateur	Accès technique réservé au service IT pour la maintenance et les incidents
Réinitialisation du mot de passe	Procédure documentée en cas d'absence prolongée ou de départ
Chiffrement avec séquestre des clés	Clés archivées séparément, accessibles au DPO en cas de besoin
Accès en présence du salarié	Modalité à privilégier pour préserver la vie privée
Procédure de départ	Transfert préalable des fichiers professionnels avant la sortie du salarié
Redirection des emails	Message d'absence et redirection temporaire des courriers professionnels
Dossiers partagés	Stockage centralisé des données professionnelles accessible à l'équipe

Pratiques et recommandations

Séparer clairement le mot de passe personnel du salarié (authentification individuelle) des droits d'administration du poste (gérés par le service IT), afin de garantir à la fois la traçabilité des actions et la continuité d'activité.

Formaliser dans la charte informatique la procédure d'accès aux données professionnelles en cas d'absence imprévue, de départ ou d'enquête interne, pour éviter toute improvisation en situation de crise.

Proscrire toute clause contractuelle ou injonction orale imposant au salarié la remise de son mot de passe personnel, car une telle exigence est contraire au RGPD et à la loyauté contractuelle.

Organiser une procédure de sortie documentée qui prévoit le transfert des fichiers professionnels par le salarié lui-même avant son départ, avec vérification par son responsable.

Consulter la délégation du personnel sur les procédures d'accès aux postes de travail, car ces mesures affectent les conditions de travail au sens de l'article L.414-1 du Code du travail.

Documenter chaque accès exceptionnel à un poste de travail en l'absence du salarié par un motif écrit, une personne habilitée et un journal horodaté, afin de pouvoir justifier la mesure en cas de contestation.

Cadre juridique

Référence	Objet
Art. L.261-1 Code du travail	Surveillance des salariés et contrôle des outils informatiques
Art. L.414-1 et s. Code du travail	Information et consultation de la délégation du personnel
RGPD, art. 5	Principes de licéité, minimisation et confidentialité
RGPD, art. 32	Sécurité du traitement et authentification
RGPD, art. 82	Droit à réparation en cas de violation
Loi du 1er août 2018	Transposition nationale du RGPD et organisation de la CNPD

Exiger le mot de passe personnel d'un salarié constitue une atteinte à la confidentialité et à la sécurité du système d'information. La bonne pratique consiste à combiner compte administrateur dédié, procédure de réinitialisation et chiffrement avec séquestre des clés pour garantir la continuité d'activité sans recourir au mot de passe du salarié.