COMMUNICATIONS ÉLECTRONIQUES ET DONNÉES ÉLECTRONIQUES

À PROPOS DE L'INSPECTION RÈGLEMENTS

KVKK_Y4 VERSION 1.00

1. OBJET ET PORTÉE

1.1. Le présent règlement a pour objet de déterminer les procédures et les principes relatifs aux conditions et au calendrier de la surveillance des communications électroniques par la Société, et ses dispositions s'appliquent au personnel et aux tiers autorisés à accéder et/ou à utiliser les installations de communication électronique de la Société.

2. SURVEILLANCE DES COMMUNICATIONS ÉLECTRONIQUES

2.1. Aux fins du présent règlement, on entend par communication électronique tous types de messages électroniques, notamment les appels téléphoniques, les télécopies, les courriels, la messagerie instantanée, les SMS et autres messages courts, les tweets, les wikis, les blogs et les contenus Web publiés sur les plateformes de messagerie. Compte tenu de la nature de ses activités, la Société n'est pas tenue de contrôler systématiquement le contenu des communications électroniques de son personnel ou de ses visiteurs. Par ailleurs, la Société ne procède pas systématiquement à un contrôle général des communications électroniques par échantillonnage aléatoire ou intervention humaine. Toutefois, un contrôle automatisé du trafic de courriels est effectué, dans une certaine mesure, afin de prévenir l'envoi massif de courriels non sollicités (communément appelés « spam ») et les contenus potentiellement dangereux (virus informatiques, tentatives de fraude financière, etc.).

2.2.5.4. Tous les utilisateurs reconnaissent qu'en utilisant les systèmes de communication électronique fournis par la Société, celle-ci ne garantit en aucun cas la confidentialité des messages ou des données stockés ou transmis par ces systèmes ; que la Société se réserve les droits énoncés dans le présent document ; et que l'utilisation de ces systèmes est limitée aux fins approuvées par la Société, lesquelles les utilisateurs ont été informés. L'utilisation des systèmes de communication électronique de la Société dans le cadre de ses activités et à des fins personnelles non essentielles ne constitue pas un droit, mais une autorisation accordée à ses employés et aux tiers autorisés.

Par conséquent, la Société peut, à tout moment et sans préavis, bloquer totalement ou partiellement l'accès à tout ou partie de ses systèmes de communication électronique et informatiques (pour tous les utilisateurs ou certains d'entre eux). Les utilisateurs des systèmes de communication électronique et informatiques de la Société sont tenus de respecter le Règlement de la Société relatif aux procédures et principes d'utilisation des technologies de l'information et de la communication, ainsi que la section 11.9 « Conditions d'utilisation acceptable des ressources informatiques (Politique d'utilisation acceptable) » de la Politique de sécurité de l'information. En utilisant ces systèmes, ils reconnaissent avoir accepté la Politique d'utilisation acceptable, s'engager à la respecter, en avoir été informés et consentir à sa mise en œuvre par la Société. Les utilisateurs s'engagent également à respecter la législation applicable et à s'abstenir de tout comportement susceptible d'engager la responsabilité de la Société. La Société peut, à tout moment et sans préavis, modifier le Règlement relatif aux procédures et principes d'utilisation appropriée d'Internet et des outils de communication électronique, ainsi que toute autre condition d'utilisation des systèmes informatiques.

Nous nous réservons le droit d'apporter des modifications et de prendre toute mesure requise ou appropriée en vertu de la législation applicable.

2.3. Conformément à l'article 6 de la loi n° 5651 relative à la réglementation des publications sur Internet et à la lutte contre la criminalité commise par le biais de ces publications, intitulé « Obligations du fournisseur d'accès », la Société prend les mesures nécessaires pour stocker les informations relatives au trafic de communications électroniques reçues ou envoyées par elle, dans la limite des finalités prévues par la loi, et pour garantir l'exactitude, l'intégrité et la confidentialité de ces informations. Ces mesures comprennent notamment la surveillance de l'utilisation des informations à des fins criminelles ou non autorisées, la réalisation d'audits et d'interventions pour protéger le système contre les menaces telles que les virus, le piratage et les attaques par déni de service, ainsi que la garantie de la conformité des opérations informatiques avec les politiques et directives de la Société.

2.4. La surveillance des communications électroniques sera principalement effectuée avec le consentement de la personne concernée. Toutefois, la Société se réserve le droit de procéder à une surveillance d'office pour atteindre ses objectifs légitimes dans les cas suivants :

2.4.1. Tenir des registres des transactions et autres communications lorsqu'il est nécessaire ou souhaitable de connaître certains éléments de la communication entre les parties concernées afin d'assurer la sécurité des activités et transactions financières et économiques ;

2.4.2. Afin de confirmer la conformité aux réglementations et pratiques concernant la Société, notamment en vérifiant si les règlements administratifs et les directives internes et les codes de conduite de la Société sont mis en œuvre ;

2.4.3. Définir ou démontrer les normes que doivent atteindre les personnes utilisant les systèmes d'information électroniques de la Société à des fins telles que le contrôle de la qualité ou la formation du personnel ;

2.4.4. Surveillance ou enregistrement pour prévenir ou détecter des actes criminels, par exemple la corruption, l'utilisation abusive de systèmes informatiques ou d'autres activités illégales.

2.4.5. Pour prévenir ou détecter l'utilisation non autorisée des systèmes d'information et de communication électroniques, par exemple pour empêcher les employés de violer les règlements de l'entreprise mentionnés dans la section 11 : « Conditions d'utilisation des ressources informatiques (Politique d'utilisation acceptable) » de la politique de sécurité de l'information ;

2.4.6. Afin d'assurer le bon fonctionnement du système en détectant et en supprimant les virus, en contrôlant et en arrêtant d'autres menaces pesant sur le système telles que le piratage ou les attaques par déni de service ; et en créant des flux réseau et des journaux de messagerie ;

2.5. Les personnes utilisant les systèmes de communication électronique de l'entreprise doivent savoir que les administrateurs des systèmes et réseaux informatiques surveillent régulièrement les transmissions et les informations transactionnelles afin de garantir le bon fonctionnement des services informatiques de l'entreprise. Dans ce cas, le personnel concerné peut accéder involontairement à des informations électroniques.

Ils peuvent avoir connaissance du contenu de la communication. Sauf disposition contraire du présent règlement ou de la législation applicable, il est interdit auxdits responsables de consulter sciemment le contenu des informations relatives aux transactions des employés de la Société ou d'utiliser de quelque manière que ce soit les informations qu'ils ont vues, entendues ou lues. Toutefois, en cas de violation des politiques et règlements administratifs de la Société ou des dispositions légales, l'infraction doit être signalée à la direction.

3. ANALYSE DES DONNÉES ÉLECTRONIQUES

3.1. La Société peut être amenée à consulter ponctuellement les courriels professionnels stockés sur des périphériques de stockage connectés au réseau ou indépendants, les documents et fichiers situés sur les lecteurs locaux, principaux ou partagés, ainsi que les données relatives aux accès aux systèmes ou bâtiments de la Société. Par ailleurs, les employés et visiteurs se connectant au réseau de la Société avec leurs appareils personnels sont réputés avoir consenti à la surveillance de leurs données aux fins spécifiées à la section 6 de la Politique de sécurité de l'information de la Société, intitulée « Surveillance des communications électroniques ». Ces audits, limités à la garantie de la sécurité des données, seront réalisés conformément aux principes énoncés dans la loi n° 6698 relative à la protection des données personnelles.

3.2. Dans des circonstances normales, la Société obtiendra le consentement de l'utilisateur avant de procéder à toute consultation de données le concernant, telles que les comptes de messagerie, les identifiants de conduite principaux ou secondaires, et les journaux d'accès. Cependant, cette consultation sera effectuée même en l'absence d'autorisation de l'utilisateur dans les cas suivants :

3.2.1. Lorsque la loi le prévoit ;

3.2.2. S'il existe des preuves crédibles allant au-delà des simples ragots ou rumeurs, et s'il existe un fort soupçon que des dispositions légales ou des politiques de l'entreprise ont pu être violées ;

3.2.3. Dans des circonstances exceptionnelles et des situations d'urgence où le fait de ne pas agir entraînerait des dommages corporels graves, des pertes ou des dommages importants aux biens, la perte de preuves importantes d'une violation de la loi ou des politiques et règlements de la Société, ou des responsabilités financières importantes pour la Société ou ses employés et/ou administrateurs ;

3.2.4. Le fait de ne pas agir peut affecter le fonctionnement administratif ou financier de la Société. si leur capacité à remplir leurs responsabilités risque d'être gravement compromise.

3.3. Si l'utilisateur concerné se trouve hors des locaux de la Société et que l'examen des données le concernant est nécessaire pour des raisons commerciales, son consentement doit être obtenu au préalable. Si l'utilisateur est injoignable, le responsable du service concerné et le directeur général peuvent autoriser par écrit la réalisation d'un audit de l'ordinateur ou des autres appareils mis à sa disposition pour les besoins de l'activité de la Société. Dans ce cas, le consentement nécessaire doit être obtenu.

Les mesures et les raisons justifiant les inspections seront consignées dans un rapport.

3.4. S'il est nécessaire de consulter des données détenues par un utilisateur ou relatives à des personnes physiques, comme indiqué à la section 3.2 ci-dessus, sans obtenir le consentement de la personne concernée, les règles suivantes s'appliquent :

3.4.1. Situations d'urgence : Les exigences minimales de la situation d'urgence peuvent être examinées et les mesures minimales nécessaires pour remédier à la situation peuvent être prises immédiatement sans autorisation ; cependant, une fois la situation d'urgence passée, une autorisation appropriée doit être demandée sans délai et la situation doit être consignée conformément au paragraphe 3.3 ;

3.4.2. Dans tous les autres cas, aucune mesure ne sera prise sans l'autorisation écrite du chef de département concerné et du directeur général.

3.4.3. Données chiffrées : Si des données chiffrées sont trouvées lors d'un audit système, la clé de déchiffrement doit être fournie sur demande.

3.4.4. Les données créées par ou concernant des employés ayant quitté l'entreprise appartiennent à cette dernière, sous réserve des délais légaux de destruction. Il n'est pas nécessaire d'obtenir l'autorisation de l'ancien employé pour consulter ces informations. L'autorisation de consultation doit être obtenue selon la procédure décrite au point 3.3 ci-dessus.

3.5. Une fois l'autorisation accordée, les données contenues dans les systèmes de la Société seront traitées comme suit : sera abordé :

3.5.1. Les documents relatifs à l'entreprise seront évalués selon les pratiques commerciales normales. Elles seront conservées ou supprimées selon les besoins.

3.5.2. Les données personnelles ne seront pas examinées sauf s'il existe une raison légitime.

3.5.3. Les employés de l'entreprise sont responsables de la suppression de leurs données personnelles contenues dans les documents électroniques et les courriels avant la fin de leur emploi.

3.6. Confidentialité : Tous les audits réalisés en vertu du présent règlement seront menés dans le respect du droit à la vie privée. Les informations relatives à la vie privée des personnes seront soumises au minimum nécessaire aux fins de l'audit. Toute information confidentielle non pertinente à l'objet de la recherche ne sera divulguée à aucun tiers et restera confidentielle. Toutefois, si des éléments illégaux ou contraires aux politiques de l'entreprise sont découverts lors des audits, le directeur général en sera immédiatement informé et des mesures seront prises conformément à ses instructions.