



RÈGLEMENT INTÉRIEUR

Mise à jour du 22 février 2023

Table des matières

Article 1.	Objet et champ d'application.....	3
Article 2.	Horaire de travail.....	3
Article 3.	Accès à l'entreprise.....	4
Article 4.	Sorties pendant les heures de travail.....	4
Article 5.	Usage du matériel de l'entreprise.....	4
Article 6.	Usage du véhicule de service.....	5
Article 7.	Usage des locaux de l'entreprise.....	6
Article 8.	Usage des systèmes d'information.....	6
Article 9.	Exécution des activités professionnelles.....	7
Article 10.	Retards, absences.....	7
Article 11.	Formation.....	7
Article 12.	Interdiction du harcèlement et des agissements sexistes.....	7
12.1	Harcèlement sexuel.....	7
12.2	Harcèlement moral.....	8
12.3	Autres dispositions relatives au harcèlement.....	8
12.4	Agissement sexiste.....	9
Article 13.	Neutralité.....	9
Article 14.	Hygiène.....	9
Article 15.	Sécurité et prévention.....	10
Article 16.	Modalité d'exercice du droit d'alerte et de retrait.....	11
Article 17.	Objets personnels.....	11
Article 18.	Discrétion et secret professionnel.....	11
Article 19.	Sanctions disciplinaires.....	11
Article 20.	Droits de la défense.....	12
Article 21.	Date d'entrée en vigueur.....	13
Article 22.	Modifications ultérieures.....	13
Annexe - Charte Informatique Groupe.....		14
Annexe - Procédure de recueil des alertes professionnelles.....		15
Annexe - Code de conduite anti-corruption.....		16

Préambule

Article 1. Objet et champ d'application

Conformément à la loi (art. L.1311-2 du Code du Travail), ce règlement fixe les règles de discipline intérieure en rappelant les garanties dont leur application est entourée et précise certaines dispositions d'hygiène et de sécurité.

Parce qu'il est destiné à organiser la vie dans l'entreprise dans l'intérêt de tous, ce règlement s'impose à chacun dans l'entreprise, en quelque endroit qu'il se trouve.

La hiérarchie est fondée à veiller à son application et à accorder les dérogations justifiées.

Les dispositions de ce règlement relatives à l'hygiène et la sécurité s'appliquent également aux intérimaires, aux prestataires de services, ainsi qu'aux stagiaires présents dans l'entreprise et de façon générale, à toute personne qui exécute un travail dans l'entreprise, qu'elle soit liée ou non par un contrat de travail avec celle-ci.

Des dispositions spéciales sont prévues en raison des nécessités de service pour fixer les conditions particulières à certaines catégories de salarié.

Elles font l'objet de notes de service, établies dans les mêmes conditions que le présent règlement dans la mesure où elles comportent des prescriptions générales et permanentes dans les matières traitées par celui-ci.

Pour qu'il soit connu de tous, le présent règlement intérieur est communiqué à chaque nouveau salarié, lors de son embauche ou de son entrée dans l'entreprise, pour qu'il en prenne connaissance. Il est également à disposition sur le réseau intranet de la société, et affiché dans les locaux.

Dispositions relatives à la discipline

Dans l'exécution de son travail, le personnel est tenu de respecter les instructions de ses supérieurs hiérarchiques, ainsi que l'ensemble des instructions diffusées par voie de notes de service et d'affichage. Tout acte contraire à la discipline est passible de sanctions disciplinaires telles qu'énumérées à l'article 19 du présent règlement.

Il doit de plus faire preuve de correction dans son comportement vis-à-vis de ses collègues et de la hiérarchie, sous peine de sanctions disciplinaires.

Article 2. Horaire de travail

Les salariés soumis à un horaire doivent respecter les horaires de travail et de pause fixés par la société conformément à l'article L. 3121-16 du Code du travail. Néanmoins, l'entreprise pourra demander au(x) salarié(s) d'effectuer des heures supplémentaires, pour les besoins du service. Toutefois, nul ne peut effectuer d'heures supplémentaires de sa propre initiative. Les demandes d'heures supplémentaires ne peuvent provenir que de la société.

Conformément à la législation en vigueur, la durée du travail s'entend du travail effectif ; ceci implique que chaque salarié se trouve à son poste, si nécessaire en tenue de travail, aux heures fixées pour le début et pour la fin du travail.

Dans le cas de travaux nécessitant une présence continue (travail en équipe, travail au sein du service informatique), le salarié ne doit pas quitter son poste sans s'assurer que son remplaçant ou successeur est présent ; s'il ne l'est pas, il doit en aviser son chef de service.

Les temps de pause ne sont pas du temps de travail effectif. Ils n'entrent donc pas dans le décompte du temps de travail.

Le temps de pause accordé pour tout salarié souhaitant prendre un café et/ou faire une pause « cigarette » (en dehors des bureaux) est autorisé selon les dispositions suivantes : Deux pauses journalières seront autorisées : une le matin et une l'après-midi. Le temps maximum accordé par pause est de 10 minutes. Les temps de pause « cigarette » et « café » ne se cumulent pas.

Les pauses ne doivent pas nuire au bon fonctionnement du service ou de l'agence, et à la satisfaction clients. Il conviendra notamment de mettre en place des permanences téléphoniques pour toute absence à l'accueil des agences.

Article 3. Accès à l'entreprise

L'entrée et la sortie du personnel s'effectuent par l'entrée principale.

Le personnel n'a accès aux locaux de l'entreprise que pour l'exécution de son contrat de travail ; il n'a aucun droit d'entrer ou de se maintenir sur les lieux du travail pour une autre cause sauf s'il peut se prévaloir :

- Soit d'une disposition légale (disposition relative aux droits de la représentation du personnel ou des syndicats notamment) ;
- Soit d'une autorisation délivrée par un membre de la société.

Il est interdit au personnel d'introduire ou de faire introduire dans l'entreprise des personnes étrangères à celle-ci, sans raison de service sauf dispositions légales particulières (intéressant les représentants du personnel et des syndicats notamment) ou sauf autorisation expresse de la société.

La société aura le droit de faire procéder à la vérification des objets dont le personnel est porteur, tant à l'entrée qu'à la sortie de l'entreprise pour des raisons de sécurité collective.

Cette vérification pourra porter sur la personne même des salariés, sur ses affaires personnelles, ainsi que dans le véhicule de société.

Le salarié sera averti de son droit de s'opposer à un tel contrôle.

Tout salarié pourra toutefois exiger la présence d'un témoin (tiers appartenant à l'entreprise ou représentant du personnel) et pourra refuser de se soumettre immédiatement aux opérations de contrôle. En cas de refus, la société pourra faire procéder à la vérification par un officier de police judiciaire compétent. Dans l'attente dudit contrôle, le salarié sera tenu de patienter sur le lieu de travail.

La fouille corporelle d'un salarié, pour des raisons de décence élémentaire, sera effectuée par une personne du même sexe.

Si les circonstances le justifiaient, notamment en cas de disparitions d'objets ou de matériels appartenant à l'entreprise, ou de suspicions, ou pour des raisons de sécurité collective, la société se réserve le droit de procéder à une vérification des objets transportés. Par conséquent, cette vérification pourra être opérée sur le véhicule personnel, dans l'enceinte de l'entreprise. Cette vérification sera effectuée dans des conditions préservant la dignité et l'intimité de la personne. Elle pourra être effectuée de manière inopinée à l'unique initiative du directeur d'établissement ou de son représentant.

Pour des raisons d'hygiène ou en cas de disparitions renouvelées d'objets ou de matériels appartenant à l'entreprise, la société peut procéder à une vérification des vestiaires dans les mêmes conditions.

L'employeur ne pourra procéder à l'ouverture de l'armoire individuelle du salarié qu'en présence ou celui-ci prévenu.

L'entrée des véhicules dans l'entreprise n'est autorisée que pendant les heures de travail. En dehors des horaires de travail, aucun véhicule n'est admis à y entrer sans autorisation expresse.

Le personnel est tenu de circuler avec une extrême prudence dans l'enceinte de l'établissement. Les panneaux et prescriptions au Code de la Route doivent être respectés.

Article 4. Sorties pendant les heures de travail

Concernant les salariés soumis à un horaire de travail, les sorties pendant les heures de travail sont subordonnées à une autorisation expresse et écrite délivrée par le responsable hiérarchique. En cas d'extrême urgence, le collaborateur devra prévenir par écrit son responsable hiérarchique (mail, sms).

Article 5. Usage du matériel de l'entreprise

Tout salarié est tenu de conserver en bon état l'ensemble du matériel qui lui est confié en vue de l'exécution de son travail (exemples : outillage, véhicule, matériel informatique, téléphone portable).

Les salariés devront informer l'employeur de toute défaillance, afin qu'il puisse intervenir rapidement et y remédier.

Les salariés ne doivent pas utiliser de matériel de l'entreprise à d'autres fins, et notamment à des fins personnelles, sauf autorisation expresse et écrite de la société et dans les limites déterminées par l'entreprise. Toute autre utilisation est interdite.

Par exemple, il est interdit :

- d'envoyer toute correspondance personnelle aux frais de l'entreprise,
- de se faire adresser des correspondances ou colis personnels à l'adresse de l'entreprise,
- d'utiliser le téléphone société à des fins personnelles, hors cas d'urgence,
- d'emporter des objets, appartenant à l'entreprise sans autorisation expresse,
- d'emporter les dossiers clients originaux hors de l'agence.

Il est formellement interdit de commercialiser ou de faire don du matériel incendie (neuf ou rebut) distribué par le groupe Eurofeu pour son compte personnel.

Il est interdit à tout salarié d'utiliser les sites de vente en ligne (internet) pour distribuer le matériel de l'entreprise.

Lors de la cessation de son contrat de travail, tout salarié doit, avant de quitter l'entreprise, restituer l'ensemble des matériels confiés (véhicule, outillage, téléphone, etc...) conformément à l'inventaire d'attribution) et récupérés dans le cadre de leur activités (rebut, organes à recycler, tout appareil récupéré chez les clients dans le cadre des activités de maintenance, etc.) et des documents en sa possession et appartenant à l'entreprise sans pouvoir en conserver ou en divulguer de copie.

Article 6. Usage du véhicule de service

Un véhicule de service peut être confié au salarié pour les besoins exclusifs de son activité professionnelle.

Il est interdit aux salariés :

- D'utiliser le véhicule de service pour ses besoins personnels ou privés (voir Annexe au contrat de travail « Mise à disposition du véhicule ») ;
- De transporter des passagers étrangers à la Société sauf dans le cadre d'activités professionnelles (clients, fournisseurs, etc.).

Les salariés qui effectuent des déplacements à l'aide de véhicules de service sont informés de l'installation de la géolocalisation (voir Annexe au contrat de travail « Mise à disposition du véhicule »).

Pendant les heures de travail, les salariés qui effectuent des déplacements doivent respecter les dispositions du Code de la Route et les réglementations en vigueur, notamment en matière de vitesse et de temps de pause.

Les salariés auxquels l'entreprise met à la disposition un véhicule de service doivent signaler à l'entreprise toute infraction qui serait commise à l'occasion de la conduite ou du stationnement dudit véhicule, tout comme les accidents de la route qui surviendraient.

Tout accident impliquant un véhicule de service doit faire l'objet d'un constat écrit, dont un exemplaire sera remis à l'entreprise, dans les 48 heures de l'accident, sauf cas de force majeure.

Le salarié est responsable du paiement des amendes occasionnées par ses infractions au Code de la Route. La Société fournira aux services compétents les renseignements permettant d'identifier l'auteur de l'infraction afin de lui imputer directement l'infraction et le règlement de l'amende au Trésor Public.

Il est rappelé, conformément aux dispositions de l'article L121-6 du Code la route que, lorsqu'une infraction constatée selon les modalités prévues à l'article L. 130-9 a été commise avec un véhicule appartenant à l'entreprise, le représentant légal de la Société doit communiquer, dans un délai de quarante-cinq jours à compter de l'envoi ou de la remise de l'avis de contravention, à l'autorité mentionnée sur cet avis, l'identité et l'adresse de la personne physique qui conduisait ce véhicule, à moins qu'il n'établisse l'existence d'un vol, d'une usurpation de plaque d'immatriculation ou de tout autre événement de force majeure.

Dans ce cadre, il est rappelé que la société a mis en place une procédure rigoureuse d'identification des conducteurs des véhicules de l'entreprise permettant la dénonciation automatique des contrevenants.

Le salarié bénéficiant d'un véhicule de service a l'obligation de prévenir immédiatement la société par courrier avec accusé de réception adressé au siège social (Parc'Auto Groupe Eurofeu - 12 rue Albert Rémy, 28250 Senonches), s'il fait l'objet d'une annulation ou d'une suspension de son permis de conduire.

La non-divulgaration par le salarié de sa suspension ou de l'annulation de son permis de conduire et/ou l'usage du véhicule de service après la mise en œuvre de cette mesure entraînera une sanction disciplinaire pouvant aller jusqu'au licenciement.

Conformément au Code de la Route, il est remis à chaque collaborateur utilisant un véhicule de service un gilet rétro-réfléchissant et un triangle de pré-signalisation. La Société décline toute responsabilité en cas de sanction suite à une non-présentation du kit de sécurité lors d'un contrôle routier.

L'usage du téléphone portable en état de conduite est strictement interdit. Il en est de même pour la consommation de stupéfiants ou d'alcool dans les limites légales.

Il est interdit de faire circuler un véhicule dont le poids dépasse son PTAC (Poids Total Autorisé à Charge).

Le salarié doit veiller à l'entretien régulier du véhicule confié. Il doit veiller à l'état de ses pneumatiques et au respect de la pression des pneus préconisée par le constructeur. Il doit informer le service Parc auto des anomalies constatées. La violation des règles expose le salarié à des sanctions disciplinaires.

Lors de chaque déplacement, tout conducteur doit s'assurer qu'il est effectivement en possession des pièces et documents concernant le véhicule et vérifier de façon systématique l'état des pneumatiques, la pression des pneus, les niveaux ainsi que le bon fonctionnement des dispositifs d'éclairage et de signalisation. Il doit immédiatement signaler toute anomalie ou défectuosité constatée ainsi que procéder aux visites d'entretien aux kilométrages prévus. Il doit signaler au responsable de service, dès le retour d'un déplacement, les incidents, accidents ou faits anormaux survenus au véhicule ou dans le fonctionnement de celui-ci.

Article 7. Usage des locaux de l'entreprise

Les locaux de l'entreprise sont réservés exclusivement aux activités professionnelles de ses salariés ; il ne doit pas y être fait de travail personnel. Il est interdit :

- D'introduire dans les lieux de travail des objets ou marchandises, destinés à y être vendus, troqués, échangés ou loués (exception pour le Comité d'Entreprise);
- De faire circuler sans autorisation de la société des listes de souscription ou de collecte ; seules la collecte des cotisations syndicales et la diffusion des publications et tracts syndicaux peuvent être faites sans autorisation, dans les conditions prévues par la loi.
- De se restaurer dans les locaux réservés à l'usage professionnel.

L'affichage sur les murs est interdit en dehors des panneaux muraux réservés à cet effet. Les affiches ou notes de service régulièrement apposées sur les panneaux de la société ne doivent pas être lacérées, détruites ou rendues illisibles.

Article 8. Usage des systèmes d'information

Le matériel informatique mis à disposition du salarié par la société, est réservé aux activités professionnelles et doit être utilisé conformément aux dispositions de la Charte Informatique en vigueur au sein du groupe figurant en Annexe aux présentes.

L'utilisation personnelle de l'ordinateur professionnel est admise pour satisfaire à des besoins impératifs de la vie quotidienne, mais doit rester raisonnable et ne pas affecter la sécurité du réseau, ni la productivité. Le salarié doit clairement identifier le caractère personnel du fichier ou de la correspondance, à défaut, elle est réputée être professionnelle.

Des durées excessives de connexions internet sur le temps de travail et à des fins non professionnelles, ainsi que des enregistrements de fichiers faisant ressortir par leur volume ou leur nombre un usage abusif affectant le travail, seront susceptibles de sanctions disciplinaires pouvant aller jusqu'au licenciement.

Un certain nombre de contrôles peuvent être effectués par le service Informatique, et ce dans le but d'améliorer l'utilisation d'Internet par le Groupe Eurofeu, la qualité de service et la sécurité du système, dans le respect du droit des personnes et des libertés individuelles, et notamment de la vie privée de chacun, conformément aux dispositions de l'article L. 1222-4 du Code du travail.

Ces contrôles peuvent inclure la vérification des sites Internet visités, la messagerie internet et les dossiers pour les fichiers qui n'auront pas été expressément spécifiés comme ayant un caractère personnel, le temps passé sur Internet, ou toute autre mesure de consommation de ressources via des outils dédiés.

Il est interdit :

- de consommer de la nourriture ou des boissons en utilisant ces équipements
- de télécharger depuis internet ou d'installer tout logiciel pour l'utiliser sur du matériel appartenant à la société (accès internet ou autres), sans accord préalable et exprès du service informatique)
- de naviguer sur des sites prohibés, tels que définis dans la Charte Informatique du groupe ;
- de divulguer des informations ou données appartenant au groupe Eurofeu ;

Le stockage des équipements et le transport des équipements portables doit contribuer au maximum à la protection de ces derniers.

Tout salarié est responsable de l'usage des outils informatiques et du réseau auxquels il a accès, dans le respect des consignes qui lui auront été transmises.

Le salarié doit respecter les règles de base en matière de sécurité :

- Mettre toujours un mot de passe lorsqu'il est demandé,
- Ne jamais prêter ou communiquer son identifiant/mot de passe,
- Éteindre son poste par arrêt logiciel et non par l'interrupteur pour terminer proprement ses sessions (hors cas de blocage technique),
- Ne jamais quitter son poste de travail en laissant accessible une session en cours (mise en veille avec mot de passe après plusieurs minutes d'inactivité),
- Ne pas laisser à disposition des supports informatiques (support de stockage, clé USB...) contenant des données sensibles.

La messagerie doit être utilisée à bon escient (pas de copies de messages aux personnes qui n'en ont pas besoin).

L'inobservation des règles définies ci-dessus pourra entraîner le prononcé de sanctions disciplinaires en fonction de la gravité du manquement commis.

Article 9. Exécution des activités professionnelles

Dans l'exécution des tâches qui lui sont confiées, chaque salarié est tenu de respecter les instructions verbales et écrites qui lui sont données par ses supérieurs hiérarchiques.

Article 10. Retards, absences

Tout retard doit être justifié auprès du chef de service ou du service du personnel. Les retards réitérés ou non justifiés peuvent entraîner l'une des sanctions prévues par le présent règlement.

L'absence pour maladie ou accident devra, sauf cas de force majeure, être justifiée dans les 48 heures par l'envoi d'un certificat médical indiquant la durée probable de l'absence. Toute absence autre que l'absence pour maladie ou accident doit être justifiée dans les 48 heures maximum, sauf cas de force majeure (événement imprévisible et indépendant de la volonté d'une personne et qui l'empêche de s'acquitter de ses engagements).

Toute absence non justifiée dans ces conditions peut faire l'objet d'une sanction. Il en est de même de toute sortie anticipée sans motif légitime ou sans autorisation (voir ci-dessus article 4), sauf pour les personnes appelées à s'absenter de façon régulière en raison de leur fonction représentative du personnel ou d'un mandat syndical.

Toute absence pour congés, RTT ou JNT, doit être préalablement et expressément autorisée par le responsable hiérarchique.

Article 11. Formation

Tout salarié est tenu de suivre les actions de formation décidées par la société (en présentiel ou e-learning) dès lors qu'elles se déroulent pendant le temps de travail, qu'elles sont financées par la société et que celle-ci les estime nécessaires à l'exercice de l'emploi. Tout refus non motivé par un motif légitime pourra être sanctionné.

Article 12. Interdiction du harcèlement et des agissements sexistes

12.1 Harcèlement sexuel

Selon les dispositions des articles L. 1153-1 et suivants du Code du travail, aucun salarié ne doit subir des faits :

- Soit de harcèlement sexuel, constitué par des propos ou comportements à connotation sexuelle répétés qui portent atteinte à sa dignité en raison de leur caractère dégradant ou humiliant, ou créent à son encontre une situation intimidante, hostile ou offensante ;
- Soit assimilés au harcèlement sexuel, consistant en toute forme de pression grave, même non répétée, exercée dans le but réel ou apparent d'obtenir un acte de nature sexuelle, que celui-ci soit recherché au profit de l'auteur des faits ou au profit d'un tiers.

Aucun salarié, aucune personne en formation ou en stage, aucun candidat à un recrutement, à un stage ou à une formation en entreprise ne peut être sanctionné, licencié ou faire l'objet d'une mesure discriminatoire, directe ou indirecte, notamment en matière de rémunération, de formation, de reclassement, d'affectation, de qualification, de classification, de promotion professionnelle, de mutation ou de renouvellement de contrat pour avoir subi ou refusé de subir des faits de harcèlement sexuel tels que définis à l'article L. 1153-1, y compris, dans le cas mentionné au 1° du même article, si les propos ou comportements n'ont pas été répétés.

Aucun salarié, aucune personne en formation ou en stage ne peut être sanctionné, licencié ou faire l'objet d'une mesure discriminatoire pour avoir témoigné de faits de harcèlement sexuel ou pour les avoir relatés.

Toute disposition ou tout acte contraire à ces dispositions est nul.

La société prend toutes dispositions nécessaires en vue de prévenir les faits de harcèlement sexuel, d'y mettre un terme et de les sanctionner, dans les lieux de travail ainsi que dans les locaux ou à la porte des locaux où se fait l'embauche.

Aucune personne ayant subi ou refusé de subir des faits de harcèlement sexuel définis à l'article L. 1153-1, y compris, dans le cas mentionné au 1° du même article L. 1153-1, si les propos ou comportements n'ont pas été répétés, ou ayant, de bonne foi, témoigné de faits de harcèlement sexuel ou relaté de tels faits ne peut faire l'objet des mesures mentionnées à l'article L. 1121-2. Ces personnes bénéficient des protections prévues aux I et III de l'article 10-1 et aux articles 12 à 13-1 de la loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique.

Dans toute entreprise employant au moins 250 salariés est désigné un référent chargé d'orienter, d'informer et d'accompagner les salariés en matière de lutte contre le harcèlement sexuel et les agissements sexistes (art. L. 1153-5-1).

Enfin, tout salarié ayant procédé à des faits de harcèlement sexuel est passible d'une sanction disciplinaire, conformément au présent Règlement, et sera informé des dispositions de l'article 222-33 du Code pénal et des peines encourues.

12.2 Harcèlement moral

Selon les dispositions des articles L. 1152-1 et suivants du Code du travail, Aucun salarié ne doit subir les agissements répétés de harcèlement moral qui ont pour objet ou pour effet une dégradation des conditions de travail susceptible de porter atteinte à ses droits et à sa dignité, d'altérer sa santé physique ou mentale ou de compromettre son avenir professionnel.

Aucun salarié, aucune personne en formation ou en stage, ne peut être sanctionné, licencié ou faire l'objet d'une mesure discriminatoire, directe ou indirecte, notamment en matière de rémunération, de formation, de reclassement, d'affectation, de qualification, de classification, de promotion professionnelle, de mutation ou de renouvellement de contrat pour avoir subi ou refusé de subir des agissements répétés de harcèlement moral ou pour avoir témoigné de tels agissements ou les avoir relatés.

Toute rupture du contrat de travail qui en résulterait, toute disposition ou tout acte contraire est nul.

Aucune personne ayant subi ou refusé de subir des faits de harcèlement moral, ou ayant, de bonne foi, relaté ou témoigné de faits de tels agissement ne peut faire l'objet des mesures mentionnées à l'article L. 1121-2. Ces personnes bénéficient des protections prévues aux I et III de l'article 10-1 et aux articles 12 à 13-1 de la loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique.

L'employeur prend toutes dispositions nécessaires en vue de prévenir les agissements de harcèlement moral. Les personnes mentionnées à l'article L. 1152-2 sont informées par tout moyen du texte de l'article 222-33-2 du code pénal (art. L. 1152-4).

Tout salarié ayant procédé à des agissements de harcèlement moral est passible d'une sanction disciplinaire.

Une procédure de médiation peut être mise en œuvre par toute personne de l'entreprise s'estimant victime de harcèlement moral ou par la personne mise en cause. Le choix du médiateur fait l'objet d'un accord entre les parties. Le médiateur s'informe de l'état des relations entre les parties. Il tente de les concilier et leur soumet des propositions qu'il consigne par écrit en vue de mettre fin au harcèlement. Lorsque la conciliation échoue, le médiateur informe les parties des éventuelles sanctions encourues et des garanties procédurales prévues en faveur de la victime.

12.3 Autres dispositions relatives au harcèlement

Selon les dispositions des articles L. 1154-1 à L. 1155-2 du code du travail :

Lorsque survient un litige relatif à l'application des articles L. 1152-1 à L. 1152-3 et L. 1153-1 à L. 1153-4, le candidat à un emploi, à un stage ou à une période de formation en entreprise ou le salarié établit des faits qui permettent de présumer l'existence d'un harcèlement. Au vu de ces éléments, il incombe à la partie défenderesse de prouver que ces agissements ne sont pas constitutifs d'un tel harcèlement et que sa décision est justifiée par des éléments objectifs étrangers à tout harcèlement. Le juge forme sa conviction après avoir ordonné, en cas de besoin, toutes les mesures d'instruction qu'il estime utiles (art. L. 1154-1).

Les organisations syndicales représentatives dans l'entreprise peuvent exercer en justice toutes les actions résultant des articles L. 1152-1 à L. 1152-3 et L. 1153-1 à L. 1153-4. Elles peuvent exercer ces actions en faveur d'un salarié de l'entreprise dans les conditions prévues par l'article L. 1154-1, sous réserve de justifier d'un accord écrit de l'intéressé. L'intéressé peut toujours intervenir à l'instance engagée par le syndicat et y mettre fin à tout moment (art. L. 1154-2).

Le fait de porter ou de tenter de porter atteinte à l'exercice régulier des fonctions de médiateur, prévu à l'article L. 1152-6, est puni d'un emprisonnement d'un an et d'une amende de 3 750 € (art. L. 1155-1).

Sont punis d'un an d'emprisonnement et d'une amende de 3 750 € les faits de discriminations commis à la suite d'un harcèlement moral ou sexuel définis aux articles L. 1152-2, L. 1153-2 et L. 1153-3 du présent code. La juridiction peut également ordonner, à titre de peine complémentaire, l'affichage du jugement aux frais de la personne condamnée dans les conditions prévues à l'article L. 131-35 du code pénal et son insertion, intégrale ou par extraits, dans les journaux qu'elle désigne. Ces frais ne peuvent excéder le montant maximum de l'amende encourue (art. L. 1155-2).

12.4 Agissement sexiste

Selon l'article L. 1142-2-1 du code du travail, nul ne doit subir d'agissement sexiste, défini comme tout agissement lié au sexe d'une personne, ayant pour objet ou pour effet de porter atteinte à sa dignité ou de créer un environnement intimidant, hostile, dégradant, humiliant ou offensant.

Tout salarié ayant procédé à de tels agissements est passible d'une sanction disciplinaire, conformément au présent Règlement.

Article 13. Neutralité

Le principe de neutralité a vocation à garantir l'égalité entre les femmes et les hommes, le respect et la compréhension de l'autre et à empêcher toute forme de discrimination et de violence.

Les salariés devront par conséquent se garder d'exprimer leurs convictions religieuses ou politiques à l'égard de toute personne qu'ils sont amenés à côtoyer à l'occasion de l'exercice de leurs fonctions (collègues de travail, clients, fournisseurs...), dans la mesure où l'expression de ces convictions porterait atteinte :

- À l'image du principe de neutralité appliqué au sein du groupe Eurofeu ;
- Au respect des règles sanitaires, d'hygiène ou de sécurité inhérentes au fonctionnement de l'entreprise ;
- Au bon fonctionnement de l'entreprise ;
- À la qualité ou à la pérennité de la relation avec la clientèle de la société.

Cet article ne fait pas obstacle à l'action syndicale.

Article 13 bis - Lanceur d'alerte

Les lanceurs d'alerte bénéficient du dispositif de protection prévu au chapitre II de la loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique.

Hygiène et sécurité

Article 14. Hygiène

Il est interdit de pénétrer ou de demeurer dans l'établissement en état d'ivresse, sous l'emprise de la drogue ou de médicaments psychotropes.

Il pourra être demandé aux salariés qui manipulent des produits dangereux, ou inflammables, ou qui sont affectés à une machine dangereuse ou qui conduisent des véhicules automobiles de se soumettre à un alcootest, un éthylotest ou à un test salivaire de dépistage de stupéfiants afin de garantir leur propre sécurité et celle de leurs collègues. Il en va de même pour les salariés dont l'état d'imprégnation alcoolique constituerait de par la nature de leurs fonctions une menace pour eux-mêmes ou pour leur entourage.

Le salarié faisant l'objet d'un tel contrôle peut demander la présence d'un tiers, représentant du personnel ou à défaut un salarié de l'entreprise, et pourra exiger une contre-expertise à la charge de l'entreprise. Il a la faculté de contester le résultat du contrôle alcoolémique et pourra alors demander à être soumis à un second contrôle alcoolémique après quelques minutes. Les personnes amenées à pratiquer le test sont tenues au secret des résultats.

En cas de refus du salarié de se soumettre à un tel test, les services de police judiciaire compétents pourront alors être alertés. Des mesures conservatoires pour assurer la sécurité des personnes et des biens pourront être mises en œuvre.

Il est également interdit d'introduire ou de distribuer dans les locaux de travail de la drogue. L'introduction ou la consommation de boissons alcoolisées dans les locaux de travail autres que le vin, la bière, le cidre et le poiré (article R.4228-20 du Code du travail) est interdite sauf dans des circonstances exceptionnelles (pots de départ ou pots organisés par l'employeur par exemple) et avec l'accord exprès de la société.

Conformément aux articles L.3511-7 et R.3511-1 du Code de la Santé Publique, il est strictement interdit de fumer dans les locaux affectés à un usage collectif ou individuel.

L'interdiction de fumer sur les lieux de travail s'applique également à l'utilisation de cigarettes électroniques.

L'interdiction de fumer s'applique dans tous les lieux fermés et couverts qui constituent des lieux de travail, y compris dans les véhicules de services.

Le personnel itinérant technicien dispose de tenues de travail conformes à la réglementation du travail. À cet effet, il a obligation de porter ces tenues et les équipements de protection individuelle mis à sa disposition et de veiller au bon état de ces équipements. En cas de défaillance d'un équipement constatée par le salarié, celui-ci doit en informer immédiatement son responsable hiérarchique.

Le personnel en contact avec la clientèle doit faire preuve de politesse et de courtoisie, et d'une hygiène parfaite.

Par ailleurs, pour des raisons évidentes d'hygiène et de sécurité, et pour la bonne marche de l'entreprise, il est également interdit aux salariés de pénétrer dans les locaux de l'entreprise avec un animal, quel qu'il soit.

Le refus du salarié de se soumettre aux obligations relatives à l'hygiène peut entraîner l'une des sanctions prévues au présent règlement. Il en est de même pour une absence non excusée à une convocation de visite médicale, le salarié ayant, par principe, l'obligation de se rendre aux visites médicales.

Article 15. Sécurité et prévention

Chaque salarié doit prendre connaissance des consignes de sécurité qui sont affichées sur les tableaux réservés à cet effet et avoir conscience de la gravité des conséquences possibles de leur non-respect.

Lorsque les tâches l'exigent, les substances et les préparations dangereuses peuvent être utilisées dans les conditions fixées par voie de notes affichées sur les tableaux réservés à cet effet.

Lorsque les tâches l'exigent, les équipements de travail et de protection individuelle doivent être utilisés, dans les conditions fixées par voie de notes affichées sur les tableaux réservés à cet effet.

Doivent notamment être utilisés, dès que nécessaires :

- Casques,
- Lunettes de protection,
- Gants,
- Chaussures de protection,
- Harnais de protection.

Le non-respect des consignes de sécurité par un salarié faisant courir un risque pour lui-même, ses collègues, ou toute personne présente sur les lieux de travail, pourra faire l'objet d'une sanction disciplinaire pouvant aller jusqu'au licenciement.

Il est interdit de manipuler les matériels de secours de l'entreprise (extincteurs, brancards, etc...) en dehors de leur utilisation normale, comme d'en rendre l'accès difficile.

Tout salarié ayant constaté une défaillance ou une anomalie dans les installations ou le fonctionnement des machines est tenu d'en informer son supérieur hiérarchique, sans délai ou à défaut, le responsable de la sécurité.

Les opérations de manutention sont réservées au personnel habilité à les faire.

Tout accident, même léger, survenu au cours du travail (ou du trajet) doit être porté à la connaissance du supérieur hiérarchique, le plus rapidement possible dans la journée même de l'accident, ou au plus tard dans les 24 heures sauf force majeure, impossibilité absolue au motif légitime.

Lorsque la santé et la sécurité paraissent compromises, les salariés peuvent être appelés à participer aux rétablissements de conditions de travail protégeant la sécurité et la santé des personnes, en fonction de leurs compétences et conformément aux notes de service de l'entreprise.

En application des dispositions légales en vigueur, le personnel est tenu de se soumettre aux visites médicales obligatoires périodiques, ainsi qu'aux visites médicales d'embauche et de reprise.

Le refus du salarié de se soumettre aux prescriptions relatives à la sécurité et aux visites médicales peut entraîner l'une des sanctions prévues au présent règlement.

Article 16. Modalité d'exercice du droit d'alerte et de retrait

Dans le cadre du droit d'alerte défini par la loi 2016-1691 du 9 décembre 2016, la Société a défini une procédure de recueil des alertes professionnelles internes applicable à compter du [date], en vue d'encourager et d'encadrer le signalement, par les salariés et les collaborateurs extérieurs ou occasionnels de l'entreprise, de faits illicites ou dangereux survenus dans l'entreprise. Ce dispositif détaillé en Annexe est complémentaire des voies traditionnelles de signalement et son utilisation constitue une simple faculté pour les salariés et collaborateurs.

Peuvent également être signalés dans le cadre de la présente procédure d'alerte des faits portant sur des conduites ou comportements contraires au Code de conduite anti-corruption du Groupe figurant également en Annexe au présent règlement intérieur.

Tout salarié qui a un motif raisonnable de penser qu'une situation de travail présente un danger grave et imminent pour sa vie ou sa santé, peut se retirer de cette situation, comme la Loi lui en donne le droit (article L 4131-1 du Code du Travail). Dans l'attente du résultat de l'enquête menée à ce sujet, le salarié sera affecté à des travaux de qualification similaire ou, en cas d'impossibilité, voisine.

Il doit en avvertir immédiatement son supérieur hiérarchique, le responsable de la sécurité ou toute personne compétente afin notamment de compléter le registre tenu à cet effet et laissé à la disposition des salariés.

La société ne peut demander au salarié de reprendre son activité dans une situation de travail où persiste un danger grave et imminent (L 4131-1 du Code du Travail). Aucune sanction, aucune retenue sur salaire ne peut être prise à l'encontre d'un travailleur ou d'un groupe de travailleurs qui se sont retirés d'une situation de travail dont ils avaient un motif raisonnable de penser qu'elle présentait un danger grave et imminent pour la vie ou la santé de chacun d'eux.

Article 17. Objets personnels

Les salariés sont responsables de la garde de leurs effets personnels.

Article 18. Discretion et secret professionnel

Le personnel employé par l'entreprise, quel que soit son statut, est tenu de garder une discrétion absolue sur tout ce qui a trait aux secrets, procédés de fabrication, listings clients, conditions tarifaires et d'une manière générale sur toute opération, projet ou décision non officialisé dont il aurait connaissance dans l'exercice de ses fonctions.

Aucun listing informatique et aucune donnée informatique sensible (disque dur, clé USB, transfert de données sur internet, etc.) ne sortira sans autorisation écrite préalable de la société.

Sanctions et droits de la défense des salariés

Article 19. Sanctions disciplinaires

Tout agissement considéré comme fautif par la société pourra, en fonction de sa gravité, faire l'objet de l'une ou l'autre des sanctions classées à l'alinéa suivant par ordre d'importance. Tenant compte des faits et circonstances, la sanction sera prise sans suivre nécessairement l'ordre de ce classement :

- Reproche verbal ou écrit,
- Rappel à l'ordre ou recadrage : observation écrite destinée à attirer l'attention du salarié sur le comportement à modifier
- Avertissement : sanction écrite destinée à avertir le salarié sur son comportement
- Blâme : réprimande écrite d'un comportement fautif
- Mise à pied disciplinaire : suspension temporaire du contrat pour une durée déterminée et sans rémunération. La mise à pied disciplinaire pourra durer jusqu'à 8 jours calendaires.
- Mutation disciplinaire : changement de poste à titre de sanction
- Rétrogradation : affectation à une fonction ou à un poste différent et de niveau inférieur

- Licenciement disciplinaire pour faute simple, grave ou lourde, avec ou sans préavis et indemnités de rupture, selon la gravité de la faute

Chacune de ces sanctions et notamment, l'avertissement sera susceptible de constituer ultérieurement une circonstance aggravante justifiant une sanction plus lourde.

Les actes de nature à troubler le bon ordre et la discipline seront sanctionnés. Sont notamment considérés comme tels, cette énumération n'étant ni limitative ni restrictive :

- État d'ivresse sur les lieux de travail ;
- Introduction ou stockage de boissons prohibées (notamment boissons alcoolisées en dehors du réfectoire) ;
- Commerce sur les lieux de travail (exception pour le Comité d'Entreprise) ;
- Violences sur les personnes ;
- Prises des repas au poste de travail ;
- Fumer dans les bureaux et lieux prohibés ainsi que dans les véhicules de société ;
- Utilisation abusive du téléphone portable portant atteinte à la prestation de travail ;
- Effectuer des travaux personnels sans autorisation de la société ;
- Adopter un comportement ou une tenue contraire aux bonnes mœurs ;
- Introduction de personnes étrangères à la société ne pouvant se prévaloir ni d'une autorisation de la société, ni des dispositions légales ;
- Détérioration du matériel et des bâtiments (notamment apposition d'inscription) ;
- Emporter sans autorisation écrite des matières premières, matériel incendie, rebuts ou objets quelconques appartenant à la société ;
- Lire, manger ou dormir pendant les heures de travail ;
- Faire, laisser faire ou susciter tout acte de nature à troubler la bonne harmonie au sein du personnel ;
- Faire un travail autre que celui qui est commandé et modifier les conditions d'exécution prescrites ;
- Séjourner dans les ateliers ou les bureaux en dehors de heures de travail, sans autorisation préalable de la société ;
- Tenir des propos injurieux ou accomplir des voies de faits ;
- Profiter délibérément d'une erreur ou omission, au préjudice de la société ou de ses clients ;
- Établir de fausses déclarations lors de l'embauche ou en cours de contrat.

Article 20. Droits de la défense

Toute sanction sera motivée. Toute sanction, hormis le reproche verbal, sera notifiée par écrit au salarié.

En outre, toute sanction, sauf si la sanction envisagée est un avertissement, une sanction moindre ou une sanction de même nature qui n'a pas d'incidence, immédiate ou non, sur la présence dans l'entreprise, la fonction, la carrière ou la rémunération du salarié, sera entourée des garanties de procédure prévues par les articles L.1332-1/L.1332-2/R.1332-1/R.1332-2/R.1332/3 du Code du Travail.

Article L.1332-1 : Aucune sanction ne peut être prise à l'encontre du salarié sans que celui-ci soit informé, dans le même temps et par écrit, des griefs retenus contre lui.

Article L. 1332-2 : Lorsque l'employeur envisage de prendre une sanction, il convoque le salarié en lui précisant l'objet de la convocation, sauf si la sanction envisagée est un avertissement ou une sanction de même nature n'ayant pas d'incidence, immédiate ou non, sur la présence dans l'entreprise, la fonction, la carrière ou la rémunération du salarié.

Lors de son audition, le salarié peut se faire assister par une personne de son choix appartenant au personnel de la société.

Au cours de l'entretien, l'employeur indique le motif de la sanction envisagée et recueille les explications du salarié.

La sanction ne peut intervenir moins d'un jour franc, ni plus d'un mois après le jour fixé pour l'entretien. Elle est motivée et notifiée à l'intéressé.

Article L. 1332-3 : Lorsque les faits reprochés au salarié ont rendu indispensable une mesure conservatoire de mise à pied à effet immédiat, aucune sanction définitive relative à ces faits ne peut être prise sans que la procédure prévue à l'article L. 1332-2 ait été respectée.

Entrée en vigueur et modifications du règlement

Article 21. Date d'entrée en vigueur

Ce règlement entre en vigueur le 10 mai 2023 ; il est préalablement affiché conformément aux dispositions du Code du Travail et déposé au secrétariat du Conseil de Prud'hommes.

Conformément à l'article L. 1321-4 du Code du Travail, ce règlement a été soumis aux membres des institutions représentatives du personnel, ainsi que pour les matières relevant de sa compétence, à l'avis du comité d'hygiène, de sécurité et des conditions de travail ; les avis émis par ces organismes ont été adressés à l'inspection du travail en même temps que deux exemplaires du présent règlement.

Article 22. Modifications ultérieures

Toute modification ou retrait d'une clause de ce règlement sera, conformément au Code du Travail, soumis à la même procédure, étant entendu que toute clause du règlement qui deviendrait contraire aux dispositions légales, réglementaires ou conventionnelles applicables à la société du fait de l'évolution de ces dernières, serait nulle de plein droit.

Fait à Senonches, le 22 février 2023



Le Président

P/ Éric HENTGÈS



Annexe - Charte Informatique Groupe



Annexe - Procédure de recueil des alertes professionnelles

Mise à jour du 22 février 2023



Annexe - Code de conduite anti-corruption

Mise à jour de janvier 2022

CHARTRE INFORMATIQUE

Règles d'utilisation des ressources informatiques et des réseaux du groupe eurofeu

La présente charte se fonde sur l'article 9 du Code civil sur le droit à la protection de la vie privée.

Article 1. Objet et champ d'application

La charte informatique a pour objet d'exposer les principales règles et précautions que tout utilisateur doit respecter et mettre en œuvre au sein du groupe EUROFEU. Elle clarifie les droits et les devoirs des utilisateurs.

La Direction des systèmes d'information (DSI) qui agit sous l'autorité de la Direction générale assure la sécurité du système d'information et met en place les outils et procédures d'administration qui doivent être portés à la connaissance de tous les utilisateurs. Elle a également pour mission de renseigner les utilisateurs concernant toutes questions relatives à l'utilisation du système d'information, que les utilisateurs sont invités à adresser directement sur le portail « Demandes et Incidents » ou par téléphone au « 0805.800.830 ».

Cette charte informatique s'applique à l'ensemble du personnel qui est tenu de s'y conformer ainsi qu'à toutes les personnes qui utilisent le réseau informatique du groupe. La présente charte constitue ainsi un code de bonne utilisation de l'ensemble des moyens et ressources informatiques et réseaux mis à disposition et a pour objet de préciser la responsabilité des utilisateurs. La charte est diffusée à l'ensemble du personnel du groupe Eurofeu.

La portée de la Charte couvre l'utilisation des moyens informatiques disponibles au sein des agences et l'emploi des ressources informatiques extérieures accessibles via le réseau Internet.

Le groupe Eurofeu met à la disposition de tout utilisateur des équipements informatiques (PC, logiciels, etc.), des moyens de communication (messageries, accès Internet, etc.) ainsi que des informations et données (base de données, images, vidéos, etc.) qui sont nécessaires à l'accomplissement de sa mission.

Article 2. Définitions

Ressources Informatiques : Désigne de façon générale les moyens informatiques ainsi que ceux auxquels il est possible d'accéder à distance, directement ou en cascade à partir du réseau administré. Ces ressources font partie du patrimoine du groupe Eurofeu. A cet égard, toute information émise ou stockée sur le poste de travail et les moyens de communication mis à sa disposition est et demeure la propriété du groupe Eurofeu.

Système d'Information : Désigne l'ensemble des ressources informatiques, réseaux, et téléphoniques du groupe Eurofeu constitué notamment des postes de travail fixes ou portables, périphériques, supports de stockage (tels que disques durs, bandes magnétiques, clés USB...), réseaux informatiques (serveurs, routeurs et connectiques), photocopieurs, téléphones, standard téléphonique, logiciels, fichiers, données, bases de données, systèmes de messagerie, systèmes d'archivage et de transmission de documents, intranet, extranet, et abonnements à des services interactifs.

Pour des raisons de sécurité du réseau, est également considéré comme faisant partie du Système d'Information du groupe le matériel personnel des utilisateurs connecté au réseau du groupe Eurofeu, ou contenant des informations à caractère professionnel concernant le groupe, ses clients et prospects ou ses partenaires.

Internet : Désigne la mise à disposition, par des serveurs locaux ou distants, de moyens d'échanges ou d'informations diverses : navigation Web, messagerie Internet, forums, etc.

Utilisateur : Désigne les personnes ayant accès ou utilisant les ressources informatiques et services Internet. Est considéré comme Utilisateur toute personne quel que soit son statut (permanents ou non, contractuel, stagiaire, consultant, partenaire, employés de sociétés prestataires, visiteurs occasionnels au sein du groupe Eurofeu, etc.), qui est amené à créer, consulter et mettre en œuvre ces ressources.

Poste de Travail : désigne le micro-ordinateur (et/ou le téléphone/smartphone) avec ses périphériques associés (écran, clavier, ...). Il dispose de lecteurs de cartes, de prises USB et d'un lecteur de DVD/CD-Rom.

Article 3. Objectifs

L'exploitation de tout système informatique en réseau suppose de la part des utilisateurs le respect d'un certain nombre de règles. Celles-ci ont pour but d'assurer la qualité des services, la sécurité et la performance des traitements, la préservation des données et leur confidentialité, ainsi que l'émission et la réception des données, le tout dans le respect des législations en vigueur.

Le raccordement d'un réseau informatique à un réseau public tel qu'Internet rend le respect des dites règles encore plus nécessaire. Ces règles complètent et explicitent celles énoncées par le législateur.

De nombreuses raisons justifient la mise en place de cette charte :

- Maintenir la sécurité du Système d'Information et limiter les risques de virus et d'intrusions
- Assurer la qualité et la performance du Système d'Information ;
- Préserver la confidentialité des données ;
- Limiter la profusion erratique des logiciels ;
- Eviter l'atteinte à des droits privatifs et respecter les droits d'auteur ;
- Réserver l'usage de l'outil à sa vraie finalité.

Étant donné le caractère novateur des réseaux et services informatiques, cette charte ne peut rester figée, des adaptations pourront lui être apportées ultérieurement.

Article 4. Les règles d'utilisation et de bon usage

Tout Utilisateur est responsable du matériel informatique mis à sa disposition pour remplir sa mission au sein de notre groupe. Il est aussi responsable de l'usage des ressources informatiques, des systèmes et des réseaux auxquels il a accès.

L'Utilisateur :

- ne doit pas modifier son poste de travail, notamment par l'ajout ou la suppression de matériels divers (lecteurs externes, graveurs, souris diverses, etc.) ;
- est responsable des informations qu'il stocke sur le disque local C ou D de son poste de travail, ces données n'étant pas sauvegardées par le service informatique. Seuls les dossiers et documents classés sur les serveurs NAS sont sécurisés ;
- ne doit pas installer lui-même de logiciels (à partir de cd-rom ou de téléchargements) ;
- ne doit pas quitter son poste de travail sans fermer ses fichiers ouverts et verrouiller sa session (mise en veille avec mot de passe) ou se déconnecter ;
- doit éteindre chaque soir son poste de travail, ou à tout autre moment de la journée lors d'une absence prolongée.

Le système d'information du groupe Eurofeu est un outil réservé exclusivement à l'activité professionnelle des utilisateurs.

Sauf exceptions expressément prévues dans la présente charte, l'utilisateur s'interdit d'utiliser le système d'information du Groupe Eurofeu à des fins étrangères à ses attributions, et s'engage notamment à :

- utiliser le système d'information uniquement comme outil lié à son activité professionnelle et non à des fins personnelles lucratives ou non, à des fins de publicité, de démarchage ou de promotion ;
- utiliser le système d'information comme un outil de communication professionnelle et non pour échanger des correspondances privées ;
- ne se connecter au système d'information qu'avec ses identifiants (couple nom d'utilisateur/mot de passe) et ses droits d'accès ;
- ne se connecter au système d'information qu'avec le matériel fourni ou autorisé par le Groupe Eurofeu ;

- ne pas se connecter à Internet sur des sites contraires à l'ordre public et aux bonnes mœurs, étant précisé que la DSI peut décider d'effectuer des « blocages machine » pour tentatives de connexion à ces sites ;
- ne pas participer à des jeux ou des paris en ligne.

Dans le strict respect des limites imposées dans la présente charte, le Groupe Eurofeu tolère une utilisation, notamment concernant l'accès à Internet à titre non professionnel.

Article 5. Règles de sécurité

L'Utilisateur ne doit pas utiliser ou essayer d'utiliser des comptes d'accès aux réseaux autres que le sien ou masquer sa véritable identité. Il est en particulier interdit d'utiliser une session ouverte par quelqu'un d'autre.

L'Utilisateur s'engage à :

- ne pas mettre à la disposition de personnes non autorisées un accès au système ;
- ne jamais désactiver l'anti-virus et s'assurer qu'il est à jour ;
- ne pas répondre aux messages en masse ou en chaîne des messageries ;
- éteindre son poste par arrêt logiciel et non par l'interrupteur pour terminer ses sessions ;
- ne jamais quitter le poste de travail en laissant une session ouverte en cours et toujours verrouiller la session ouverte en cours ;
- ne pas laisser à disposition des supports informatiques (cdrom, ...) contenant des données confidentielles, dans un bureau ouvert ;
- éteindre son poste de travail chaque soir lors de son départ des locaux du Groupe Eurofeu ;
- protéger les données dont l'utilisateur est responsable, en utilisant les moyens de sauvegarde mis à sa disposition ;
- respecter la confidentialité des informations relatives au Groupe ;
- ne pas extraire et consulter les données confidentielles du Groupe Eurofeu dans les lieux publics ;
- ne pas perturber le bon fonctionnement du système d'information en participant par exemple à des activités accaparant fortement les ressources partagées (impressions de gros documents, utilisation intensive du réseau ...) qui devront être effectuées aux moments qui pénalisent le moins l'ensemble des utilisateurs ;
- ne pas connecter sur le réseau du Groupe Eurofeu un ordinateur externe sans un contrôle préalable du poste par les équipes de maintenance du système d'information de la DSI et sans vérification des anti-virus à jour ;
- ne pas installer ni faciliter l'installation par un tiers, de logiciels ou de matériels informatiques n'appartenant pas au Groupe Eurofeu et sans autorisation de la DSI (ordinateur portable, smartphone, tablettes) ;
- signaler sans délai à la DSI tout incident de sécurité ou dysfonctionnement du système d'information qu'il serait amené à constater ou à subir (virus, destruction, vol, anomalie concernant les droits d'accès).

Il est en outre demandé à tout utilisateur, en particulier concernant l'utilisation des imprimantes connectées au réseau informatique du Groupe Eurofeu :

- de privilégier les impressions en mode recto/verso ;
- de privilégier de façon quotidienne les impressions en noir et blanc et limiter les impressions couleur aux seuls documents nécessitant ce traitement ;
- ne pas oublier de récupérer, sur les fax, imprimantes ou photocopieurs, les documents sensibles que l'on envoie, imprime ou photocopie ;
- de conserver les documents et archives confidentiels dans un endroit sécurisé; de ne pas laisser sur leur bureau des documents confidentiels ;
- de privilégier les broyeurs de documents pour la destruction des impressions «sensibles» et/ou confidentiels.

Article 6. Règles de confidentialité

6.1 Accès et confidentialité

Un employé devient utilisateur du système informatique à partir du moment où il a reçu du service informatique un droit d'accès (nom d'utilisateur et mot de passe).

Chaque Utilisateur est responsable des actions réalisées sous ses droits d'accès de telle sorte que ces droits d'accès ne doivent jamais être divulgués, même temporairement, à un autre utilisateur ou à tous tiers. Réciproquement, les utilisateurs ne doivent pas utiliser des droits d'accès autres que les leurs.

Le Groupe Eurofeu se réserve le droit de retirer ces droits d'accès à tout moment et notamment lors de la cessation, même provisoire, de l'activité professionnelle d'un utilisateur au sein du Groupe Eurofeu. De même que l'entreprise pourra accéder aux mails professionnels du collaborateur en cas d'absence prolongée (à l'exception des emails clairement identifiés comme personnels).

Il est interdit de prendre connaissance d'informations détenues par d'autres utilisateurs, quand bien même ceux-ci ne les auraient pas explicitement protégées. Cette règle s'applique également aux conversations privées de type courrier électronique dont l'utilisateur n'est destinataire ni directement, ni en copie.

Les informations confidentielles contenues dans le Système d'information ne doivent pas être transférées à l'extérieur du Groupe Eurofeu, que ce soit par le réseau Internet ou par copie sur un média quelconque et sur quelque support que ce soit.

En particulier, chacun doit veiller à ne pas faire sortir en dehors des locaux du Groupe Eurofeu des documents confidentiels non protégés par un mot de passe ou en limiter le déplacement ou le stockage des versions imprimables.

6.2 Mot de passe

Le mot de passe est personnel et incessible. Il ne doit pas être communiqué à un tiers. L'utilisateur ne doit pas chercher à acquérir le mot de passe d'un autre utilisateur. En cas de départ d'un utilisateur, il est de la responsabilité de l'utilisateur et de sa hiérarchie d'assurer la transmission des documents de travail et des mails, la DSI n'ayant pas connaissance du mot de passe.

Les utilisateurs seront informés au plus tôt en cas de réinitialisation de leurs mots de passe par la DSI.

L'utilisateur choisit des mots de passe sûrs et gardés secrets. Il change de mot de passe régulièrement.

La confidentialité des données véhiculées sur Internet n'est pas garantie.

Les droits d'accès sur les dossiers accessibles par le réseau sont attribués par la DSI, selon les instructions données par le Directeur du service concerné, selon les règles d'utilisation et la vocation des différents serveurs.

Article 7. Respect des outils informatiques et téléphoniques

Du matériel informatique et téléphonique est mis à disposition des utilisateurs. Chaque utilisateur est responsable du bon usage et de l'état du matériel mis à sa disposition. Exemple : nettoyage du clavier, souris, écran...

Lorsqu'un utilisateur quitte le Groupe Eurofeu, il doit restituer le matériel mis à sa disposition.

Il est strictement interdit de déplacer, d'échanger du matériel informatique ou téléphonique, ou de déplacer les connexions réseaux vers d'autres prises.

L'intégrité des données partagées par les utilisateurs sur le réseau informatique doit être respectée.

Article 8. Utilisation des logiciels

L'installation et/ou l'utilisation de logiciels autres que ceux recommandés et autorisés par le service informatique sont interdites.

Il est totalement illégal de faire des copies d'un logiciel commercial, ainsi que de contourner les restrictions d'utilisation d'un logiciel.

Tout utilisateur est responsable de l'utilisation des ressources informatiques. Chaque utilisateur doit éviter toute situation conduisant à introduire, intentionnellement ou non, des données ou applications pouvant propager des virus dans le système d'information.

Article 9. Usage de la messagerie

L'utilisation de la messagerie est réservée à un usage professionnel. L'utilisation du courrier électronique à des fins personnelles est tolérée dans des proportions raisonnables et à la condition de ne pas affecter le trafic normal des messages professionnels.

Chaque utilisateur doit veiller à prendre connaissance régulièrement du contenu de sa messagerie.

Le Groupe Eurofeu n'est en aucun cas responsable des erreurs et de la fiabilité des informations qui sont contenues dans les mails.

Les adresses électroniques fonctionnelles ou de service sont utilisables en interne ou à l'extérieur du Groupe.

Il est cependant interdit :

- d'utiliser des adresses de messagerie autres que celles attribuées par la DSI à titre professionnel ;
- d'envoyer des courriers électroniques contraires à l'ordre public ou des messages diffusant des informations fausses, erronées, tendancieuses, diffamatoires, injurieuses ou couvertes par le secret et diffusées sans l'autorisation de leur légitime propriétaire ou dépositaire ;
- d'envoyer (indirectement ou directement) des informations à caractère personnel, concernant des individus et notamment leur vie privée ;
- diffuser des œuvres protégées par les droits d'auteur.

Par ailleurs, conformément à l'article 9 du code civil, il n'est pas possible de prendre connaissance des messages personnels émis et reçus par le salarié grâce à l'outil informatique mis à disposition par l'employeur.

La messagerie est destinée à la transmission de messages et de documents facilitant la communication, à la préparation de dossiers et de notes, à l'organisation de réunions, aux échanges de documents, etc.

La transmission par la messagerie doit respecter les procédures de contrôle, de validation et d'autorisation.

Seuls les responsables ayant reçues une délégation en bonne et due forme sont compétents pour prendre des décisions au nom du Groupe Eurofeu. Les utilisateurs devront donc être particulièrement vigilants à ne pas s'engager contractuellement par courriel car ils seront engagés personnellement sans la protection du Groupe.

Il est fortement conseillé :

- de conserver tous les messages envoyés ou reçus qui peuvent avoir une valeur probatoire (impression au format PDF) ;
- de supprimer rapidement tous les messages volumineux et sans valeur contractuelle ;
- d'archiver régulièrement votre boîte aux lettres (par exemple une fois l'an) ;
- de détacher les pièces jointes et de les enregistrer ;
- d'éviter d'envoyer des messages comportant des pièces jointes trop volumineuses ;
- La taille maximale admise pour les fichiers envoyés par la messagerie doit être inférieure à 10 Mo.

Pour les fichiers plus volumineux, les utilisateurs sont informés :

- qu'il existe d'autres solutions (partage de répertoires sur les serveurs bureautiques, échanges ftp, ainsi que tous autres moyens techniques de transferts de fichiers) et qu'elles doivent être mises en œuvre chaque fois que cela est rendu nécessaire ;
- que les abonnements contractés (newsletters) doivent exclusivement être à caractère professionnel ;
- qu'avant tout envoi, il est impératif de vérifier l'identité des destinataires du message et de leur qualité à recevoir communication des informations transmises ;
- qu'en cas d'envoi à une pluralité de destinataires, l'utilisateur doit respecter les dispositions relatives à la lutte contre l'envoi en masse de courriers non sollicités (spams) ;
- qu'en cas de doute sur la qualité d'une pièce jointe reçue par la messagerie, à immédiatement contacter la DSI et de ne pas ouvrir le fichier à risques.

Par ailleurs, l'utilisateur doit utiliser avec discernement les listes de diffusion personnelles ou collectives. Il doit éviter l'envoi de copies à un nombre injustifié de destinataires.

Enfin, il est rappelé que les messages électroniques transitent par le Web et peuvent donc, à tout moment être interceptés, visualisés, enregistrés et utilisés à d'autres fins par un tiers.

9.1 Règle de sécurité

Lors de la réception d'un courrier électronique, il faut s'assurer qu'il ne contient aucun virus. Il convient tout particulièrement de se méfier des messages dont l'expéditeur est inconnu.

Ces messages ne doivent pas être ouverts. Ils doivent être immédiatement supprimés. Il est important de signaler à la DSI la réception de ce type de message.

9.2 Envoi de messages et pièces jointes

Il est nécessaire d'éviter d'envoyer des messages avec des fichiers joints de taille trop importante.

9.3 Modification ou suppression d'une boîte aux lettres

En cas de départ, d'arrivée, de changement de service ou de poste d'un collaborateur dans le Groupe, la DSI devra être informée de l'événement 10 jours au préalable par la direction du service concerné. De même, en cas de changement de nom (ex : mariage), une demande devra être adressée à la DSI pour conserver ou modifier l'adresse de messagerie. Ces dispositions sont identiques pour la création, modification ou suppression des profils informatiques et téléphoniques.

Article 10. Usage de l'Internet

La capacité de trafic sur le réseau est une ressource coûteuse et limitée. Nul ne peut accaparer à son usage, même pour un motif légitime, une ressource ayant vocation à être partagée. Pour assurer un équilibre optimal de la charge du réseau, un partage équitable de la bande passante doit être réalisé afin d'assurer des performances satisfaisantes pour tous. Il est notamment recommandé de ne pas écouter la radio depuis Internet, et de surcroît de regarder des chaînes de télévision.

L'utilisation d'Internet à des fins privées est tolérée dans des limites raisonnables et à condition que la navigation n'entrave pas l'accès professionnel.

L'utilisateur doit, en toutes circonstances et particulièrement sur Internet, ne pas contrevenir à son obligation de neutralité et faire preuve de modération, loyauté et discrétion à l'égard du Groupe Eurofeu, des utilisateurs et à tout tiers de manière générale.

C'est pourquoi l'utilisateur s'engage à respecter les lignes directrices suivantes :

- ne pas consulter les sites Internet dont le contenu serait contraire à l'ordre public et aux bonnes mœurs ou à l'intérêt, l'organisation, l'image et la réputation du Groupe Eurofeu ;
- ne se livrer en aucun cas à une activité susceptible de causer au Groupe Eurofeu un quelconque préjudice de quelque nature que ce soit, en utilisant son système d'information ;

- ne pas se livrer à des actions mettant sciemment en péril la sécurité ou le bon fonctionnement des serveurs auxquels il accède ;
- ne pas usurper l'identité d'un utilisateur et/ou intercepter de communications électroniques ;
- ne pas proposer ou rendre accessible aux tiers des données et informations confidentielles du Groupe Eurofeu ou contraires à la législation en vigueur ;
- ne pas consulter et/ou diffuser un contenu sur Internet relevant du droit pénal et susceptible de tomber sous le coup d'une infraction, d'un crime ou d'un délit (tels que l'injure, la diffamation, la pornographie, la pédophilie, l'incitation à la violence ou à la haine, discrimination sexuelle, etc.) ;
- ne pas porter atteinte à des Droits de Propriété Intellectuelle ;
- ne pas participer à des jeux de hasard, d'argent ou de s'impliquer dans le blanchiment d'argent au moyen d'Internet.

Dans le cadre de la tolérance d'un accès responsable et raisonnable à Internet à titre non professionnel, l'utilisateur ne doit pas utiliser le système d'information d'une façon susceptible de constituer un comportement illicite, en ce comprenant, de manière non limitative :

- la divulgation d'informations confidentielles relatives au Groupe Eurofeu ou à tous tiers, auxquelles l'utilisateur aurait eu accès ;
- la diffusion de « spams » ;
- la diffusion de messages à caractère injurieux, diffamatoires, pornographiques, discriminants, ou attentatoires à la vie privée ;
- l'intrusion non autorisée dans un système d'information et de façon générale toutes infractions aux articles 323-1 et suivants du Code pénal ;
- tout comportement de nature à nuire à l'intégrité et la sécurité du Système d'information du Groupe Eurofeu ;
- l'utilisation, la reproduction et la diffusion non autorisée d'éléments protégés par des Droits de Propriété Intellectuelle, appartenant au Groupe ou à tout tiers, susceptibles de constituer des actes contrefaisants au sens du Code de la propriété intellectuelle.

En toutes hypothèses, l'utilisation à titre extraprofessionnel ne doit jamais altérer ni entraver une utilisation professionnelle du système d'information, ou empêcher la réalisation des tâches professionnelles incombant aux utilisateurs

Article 11. Analyse et Contrôle

Dans le respect des principes de transparence et de proportionnalité, l'attention des utilisateurs est attirée sur le fait que les dispositifs de sécurité informatique mis en place par le Groupe Eurofeu enregistrent les traces d'activités des systèmes, rendant possible leur analyse a posteriori.

Pour des raisons de sécurité, de maintenance et de gestion technique, le Groupe Eurofeu se réserve ainsi le droit de :

- Vérifier le trafic informatique entrant et sortant ainsi que le trafic interne ;
- Dilligenter des audits pour vérifier que les consignes d'usage et les règles de sécurité et de sûreté sont correctement appliquées par les utilisateurs ;
- Contrôler l'origine licite des logiciels installés ;
- Filtrer les adresses électroniques des sites non autorisés par le Groupe Eurofeu ;
- Conserver des fichiers journaliers (« logs ») des traces de connexion Internet globales pendant une période d'une année à compter de la connexion.

L'utilisateur doit être informé que l'utilisation de la messagerie électronique laisse des traces et est nécessairement mémorisée. Les serveurs de messageries ou bureautiques font en outre l'objet de sauvegardes régulières qui permettent généralement de retrouver sur une période de 3 mois les données qui ont été stockées. La DSI assure la confidentialité des enregistrements.

Les serveurs de messageries ou bureautiques font en outre l'objet de sauvegardes régulières qui permettent généralement de retrouver sur une période de 3 mois les données qui ont été stockées. La DSI assure la confidentialité des enregistrements.

Conformément à la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, Le Groupe Eurofeu s'engage à respecter les droits d'accès et de rectification des utilisateurs concernés.

De plus, l'utilisateur est expressément informé que la DSI se réserve le droit d'exploiter ces enregistrements pour rechercher la cause d'anomalies ou de dysfonctionnements et dégradations de performance.

Si l'analyse de ces éléments laissent fortement présumer qu'il y a violation des règles définies dans la présente charte, des textes légaux ou des usages en vigueur, le Groupe Eurofeu pourra d'une part exiger de l'utilisateur concerné qu'il se justifie de sa conduite et d'autre part prendre toute mesure légale de nature à établir la faute ou le comportement fautif de l'intéressé dans les limites des règles et sanctions mises en place par le règlement intérieur du Groupe Eurofeu.

La mise en place de ces dispositifs n'a pas pour objet le contrôle individuel des utilisateurs, et nous vous informons que la confidentialité des messages sera respectée.

Article 12. Contrôle et surveillance de l'Internet

Le Groupe Eurofeu se réserve le droit de surveiller à tout moment l'utilisation faite de l'Internet et d'opérer une trace des accès faits par ses employés (fichiers de journalisation), ceci en conformité avec la CNIL, les lois en vigueur et après validation par le Comité technique.

Ces fichiers de journalisation sur la fréquentation par les utilisateurs permettent d'identifier et d'enregistrer toutes les connexions (ou tentatives) via internet. Ils ont pour finalité de garantir une utilisation normale des ressources et d'assurer l'intégrité du réseau.

Des audits du contenu des dossiers réseau des utilisateurs et des disques durs des postes informatiques pourront également être effectués pour des besoins de sécurité (anti-virus, présence de programmes en violation des droits de copyright, à caractère répréhensible ou de logiciels piratés).

Ces contrôles se feront dans le respect de la législation applicable et notamment de la loi sur l'informatique et les libertés.

Seuls les administrateurs du réseau sont autorisés à accéder aux informations enregistrées. Ceux-ci sont tenus au secret professionnel et ne peuvent divulguer les informations collectées.

Si des infractions sont commises, l'administrateur en informera la Direction générale des services, qui pourra décider d'appliquer des sanctions en vertu des lois en vigueur.

Le contrôle exercé ne porte atteinte en aucun cas à la vie privée ni à l'image des employés.

Les informations recueillies pour la création de profils informatiques ou téléphoniques et pour la constitution du fichier de journalisation des accès Internet, sont nécessaires pour maintenir la sécurité et la cohérence du système d'information. Elles font l'objet d'un traitement destiné à l'administrateur réseau et la Direction générale des services.

Conformément à la loi informatique et libertés du 6 janvier 1978, chaque utilisateur bénéficie d'un droit d'accès et de rectification aux informations qui le concernent. Si l'employé souhaite exercer ce droit et obtenir communication des informations le concernant, il peut le demander auprès du Directeur des Systèmes d'Information.

Les informations demandées pour la création des profils sont les suivantes :

- Nom, prénom et fonction ;
- Site et bureau dans lequel la personne sera installée ;
- Besoin d'une boîte mail ;
- Besoin d'un compte Dynamics AX ;
- Liste des équipements souhaités (Ordinateur portable, téléphone fixe, éventuellement smartphone, etc...) ;
- Autorisations (lecture, écriture) sur les répertoires de la direction concernée et/ou sur le portail Groupe ;

- Liste des applications devant être installées sur l'ordinateur (Skype Entreprise, Autocad, etc...).

Article 13. Contrôle et surveillance de la téléphonie

L'utilisation du réseau téléphonique à des fins privées est en principe interdite. Une tolérance est toutefois admise à l'utilisation du téléphone à des fins privées, notamment pour des appels locaux et dans le respect du bon sens.

Les personnels équipés de téléphones mobiles sont responsables de l'appareil qui leur est confié.

Chaque personne équipée s'engage à ne pas laisser le téléphone dans un véhicule (même fermé à clef) ou sans surveillance, même pour une courte durée et à ne pas le prêter à une autre personne.

Chaque personne est informée que le forfait mensuel utilisateur qui lui est attribué est réservé uniquement à une utilisation professionnelle et sur le territoire français. Les services supports du groupe Eurofeu doivent être prévenus de tout besoin de contact à l'étranger ou en cas de déplacement à l'étranger pour pouvoir prendre les précautions adéquates concernant les options à mettre en place sur le forfait. Au-delà de la durée du forfait, la Direction générale se réserve la possibilité d'enquêter et d'étudier les suites à donner.

Le bénéficiaire du téléphone portable professionnel s'engage à :

- Être l'unique utilisateur ; ne pas le prêter à une autre personne ;
- utiliser le téléphone portable uniquement dans l'hypothèse où un téléphone fixe n'est pas à proximité ;
- Appeler vers les numéros fixes en priorité ; ne pas composer de numéros spéciaux (118 218, 3635 etc.) ;
- Conserver en permanence le téléphone dans un endroit sécurisé et ne jamais le laisser sans surveillance. Ne pas le laisser dans un véhicule (même fermé à clé) ;
- Ne pas utiliser le téléphone au volant de son véhicule (même avec un kit mains libres) ;
- Informer la DSI immédiatement en cas de dysfonctionnement, de perte, de vol (dépôt de plainte obligatoire) ou de blocage de l'appareil ;
- Restituer l'appareil sur simple demande de la DSI.

Entretien : La DSI remplacera ou réparera l'appareil en cas de dysfonctionnement. Seule la Direction générale pourra décider de la date du renouvellement de l'appareil.

Contrôle : La DSI procédera aux contrôles des appels passés. Chaque responsable de service pourra exiger des explications du bénéficiaire en cas d'utilisation abusive non professionnelle.

Propriété : Le Groupe EUROFEU étant le seul propriétaire du téléphone, il se réserve le droit à tout moment de le récupérer sans préavis. Le numéro de téléphone lié au matériel est professionnel et ne pourra à aucun moment être revendiqué par le salarié, y compris en cas de changement de service.

Article 14. Sanctions applicables

Ce document est fondé sur le respect traditionnel des droits et des devoirs des collaborateurs dans le cadre de leurs missions au sein du groupe Eurofeu afin d'éviter que l'utilisation des moyens informatiques ne se retourne contre eux ou contre le groupe lui-même.

L'objet de la présente charte est d'informer chaque utilisateur sur les règles à suivre lors de l'utilisation du système d'information du Groupe Eurofeu dans les meilleures conditions de sécurité, de performance et de confidentialité tant dans les intérêts du groupe que pour les utilisateurs eux-mêmes.

Article 15. Sanctions internes

Les utilisateurs ne respectant pas cette charte sont passibles de procédures disciplinaires internes.

De plus, pour des raisons de continuité de service, il peut être demandé à un utilisateur qui quitte le Groupe Eurofeu, d'autoriser par écrit l'accès à sa messagerie professionnelle et à ses documents après son départ de la société.

Seront sanctionnées toutes consommations abusives des téléphones, à l'évidence sans rapport avec le cadre professionnel. En cas d'abus avéré et reconnu par l'utilisateur, le Groupe Eurofeu pourra alors :

- demander un remboursement des communications privées, sur la base d'un état établi contradictoirement avec l'utilisateur ;
- sanctionner disciplinairement le collaborateur concerné.

Article 16. Poursuites pénales et civiles

L'attention de l'utilisateur est attirée sur les poursuites pénales et civiles dont lui-même, son chef de service, voire le Groupe Eurofeu pourraient faire l'objet du fait de la diffusion, par quelque moyen que ce soit, de messages répréhensibles captés sur le réseau Internet, ou de l'utilisation, de la diffusion, voire du simple enregistrement informatique d'oeuvres ou de données, en contravention avec les lois en vigueur.

Article 17. Droit à la déconnexion

Les technologies de l'information et de la communication (TIC) font désormais partie intégrante de l'environnement de travail et sont nécessaires au bon fonctionnement de l'entreprise. Ces outils permettent notamment une connexion à l'entreprise à tout moment et en tout lieu.

Si elles favorisent la flexibilité, l'efficacité du travail et le lien social, en facilitant les échanges et l'accès à l'information, elles doivent toutefois être utilisées raisonnablement et dans le respect des personnes et de leur vie privée.

À cet effet, l'ensemble du personnel de l'entreprise devra faire en sorte que l'usage de la messagerie électronique ne se substitue pas au dialogue direct et aux échanges verbaux, qui contribuent au lien social au sein de l'entreprise.

Par ailleurs, les salariés bénéficient d'un « droit à la déconnexion » en dehors de leurs périodes habituelles de travail. Par conséquent, les salariés ne sont pas tenus d'utiliser les équipements informatiques ou téléphoniques mis à leur disposition par l'entreprise dans le cadre de leurs fonctions, ni d'utiliser les connexions à distance pour se connecter aux équipements informatiques de l'entreprise ou d'échanger des messages téléphoniques ou électroniques pendant les périodes de repos journalier ou hebdomadaire ou pendant les jours de congés payés et de repos, sous réserve d'impératifs exceptionnels nécessitant une disponibilité ponctuelle.

Ainsi, les salariés ne seront pas tenus de répondre aux emails ou messages professionnels adressés pendant leurs périodes de repos, sauf durant les périodes d'astreinte et en cas d'impératifs exceptionnels nécessitant une disponibilité ponctuelle.

Plus généralement, les salariés ne pourront pas se voir reprocher la non-utilisation des outils permettant une connexion à distance et l'utilisation par les salariés de ce droit à la déconnexion ne sera pas prise en compte dans le cadre de l'évaluation de leurs performances et ne pourra pas donner lieu à d'éventuelles sanctions disciplinaires.

Article 18. Protection des données personnelles

18.1 Comment le groupe Eurofeu traite-t-il les données personnelles ?

Dans le cadre de ses activités, le groupe Eurofeu, représenté par la société AER Holding, société par actions simplifiée au capital de 4.968.112 euros dont le siège est situé à La Motte, 28250 Le Mesnil-

Thomas, immatriculée au Registre du commerce et des sociétés sous le numéro 353 207 707 RCS CHARTRES et l'ensemble de ses filiales au sens de l'article L. 233-1 du Code de commerce (ci-après le « **Groupe Eurofeu** ») collectent et traitent pour leur compte des données à caractère personnel de leurs salariés, clients, prospects, sous-traitants, prestataires ou partenaires divers.

Le Groupe Eurofeu s'engage ainsi à ce que la collecte et le traitement de toutes données personnelles, soient conformes à la loi Informatique et Libertés (Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés) et au Règlement Général sur la Protection des Données Personnelles, dit « RGPD » (Règlement n°2016/679). Ce texte a instauré un nouveau cadre européen concernant le traitement et la circulation des données à caractère personnel.

Dans le cadre de son activité, le groupe Eurofeu est amené à collecter et traiter les données suivantes :

- les données personnelles des salariés de l'entreprise,
- les données personnelles transmises dans le cadre de la relation commerciale avec un client ou un fournisseur.

Notre Politique de protection des données personnelles décrit la manière dont le Groupe Eurofeu, à travers ses différentes filiales, utilise, traite et protège vos données personnelles, ainsi que les raisons pour lesquels nous traitons ces données. La Politique de protection des données personnelles fait également partie intégrante des Conditions Générales de vente, d'achat et d'utilisation de nos produits et services.

Liste des traitements : Le Groupe Eurofeu tient à jour la liste des traitements qui utilisent les données personnelles afin que l'ensemble des propriétaires des données puissent être informés de l'utilisation faites de leurs données.

La présente Politique de Protection ne s'applique qu'aux seuls traitements de données à caractère personnel pour lesquels le Groupe Eurofeu intervient en qualité de responsable de traitement. Dans ce cadre, le traitement de données à caractère personnel peut être directement mis en œuvre par le Groupe Eurofeu ou par le biais d'un sous-traitant spécifiquement désigné par lui.

Sécurité : Il appartient au Groupe Eurofeu de définir et de mettre en œuvre les mesures techniques de sécurité ou physique, qu'il estime appropriées pour lutter contre la destruction, la perte, l'altération ou la divulgation non autorisée des données de manière accidentelle ou illicite. Parmi ces mesures figurent principalement :

- L'utilisation de mesures de sécurité pour l'accès aux locaux (fermeture des bureaux, badges, etc.) ;
- La sécurité de l'accès à nos postes informatiques et smartphones (mots de passe modifiés régulièrement) ;
- La mise en place de login et password pour toutes nos applications métiers ;
- La gestion des habilitations pour l'accès aux données (spécificité pour nos services financier et comptable et communication) ;
- Utilisation de VPN dans le cadre des connexions à distance ;
- Emploi du mot de passe complexe pour notre réseau Wi-Fi modifié régulièrement.

En tout état de cause, le Groupe Eurofeu s'engage, en cas de changement des moyens visant à assurer la sécurité et la confidentialité des données à caractère personnel, à les remplacer par des moyens d'une performance supérieure. Aucune évolution ne pourra conduire à une régression du niveau de sécurité.

Vos droits : Conformément à la réglementation en vigueur, vous disposez des droits suivants en votre qualité de salarié, de client ou de fournisseur du groupe Eurofeu :

- droit d'accès et de rectification ;
- de mise à jour, de complétude des données ;
- droit de verrouillage ou de suppression des données à caractère personnel, lorsqu'elles sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite ;
- droit de retirer à tout moment un consentement ;
- droit à la limitation du traitement des données des Utilisateurs ;
- droit d'opposition aux traitements des données personnelles ;
- droit à la portabilité des données fournies, lorsque ces données font l'objet de traitements automatisés fondés sur le consentement ou un contrat.

En qualité de propriétaire de vos données personnelles, vous pouvez obtenir des informations supplémentaires sur les données conservées et traitées par le groupe Eurofeu vous concernant en contactant le responsable des données personnelles « Data Protection Officer » du groupe Eurofeu à l'adresse suivante : dpo@eurofeu.fr ou par courrier RAR à l'adresse : DPO Groupe Eurofeu, 12 rue Albert Rémy, 28250 Senonches.

Vos demandes seront traitées sous 30 jours. En complément de votre demande, nous vous demanderons de joindre une photocopie d'un justificatif d'identité afin que le DPO puisse vérifier votre identité.

Vous pouvez vous opposer au traitement de vos données personnelles ou révoquer votre accord donné à ce traitement à tout moment. Si vous souhaitez révoquer votre accord, merci de contacter le Responsable des Données Personnelles en lui indiquant votre demande.

Si vous avez des réclamations d'une autre nature relativement au traitement de vos données personnelles par Eurofeu, vous pouvez également contacter la Commission Nationale Informatique et Liberté.

18.2 Gestion des données personnelles des salariés du groupe Eurofeu

Afin de se conformer aux exigences du Règlement Européen 2016/679, la gestion des données personnelles des salariés du groupe Eurofeu est soumise aux dispositions ci-dessous :

Objet et modalités du Traitement de vos données personnelles : Dans le cadre de votre contrat de travail, afin d'assurer la gestion administrative de votre emploi, l'employeur peut collecter pendant la durée de votre contrat des données personnelles vous concernant.

Vous trouverez ci-dessous une description des données personnelles que l'entreprise va collecter et traiter à votre sujet ainsi que la finalité et les modalités de traitement de ces données personnelles.

L'employeur peut être amené à collecter et traiter des données relatives à votre situation administrative (telle que vos nom, prénom, adresse, numéro de sécurité sociale, date et lieu de naissance, situation familiale, coordonnées bancaires), contractuelle (telle que la date de début et de fin de contrat, les conditions contractuelles, fiches d'aptitude, médecine du travail, sanctions, lettre de licenciement ou de démission et motif de licenciement, notification de maladie et toute autre information liée à votre emploi et à sa réalisation au sein du groupe Eurofeu) ou tout autre document vous concernant et nécessaire à la gestion de votre relation de travail avec le groupe Eurofeu.

Finalités de la collecte et du traitement des données personnelles :

- assurer la gestion administrative et financière de la relation de travail,
- gérer votre développement personnel et votre carrière, y compris les formations (et tout stage ou test requis à ce titre),

- se conformer aux règles de gouvernance et aux procédures internes du Groupe Eurofeu, y compris les contrôles internes, la politique de santé et sécurité au travail, les enquêtes de satisfactions salariés et toutes autres enquêtes ou audit.

En vue de ces finalités et en respect des obligations légales et réglementaires, l'Employeur peut notamment collecter et traiter les données suivantes : Nom, Prénom, adresse, numéro de sécurité sociale, titre, e-mail, noms d'utilisateur et mots de passe, curriculum-vitae, formations, tests, validation d'acquis professionnel et toutes données requises par la loi.

L'Employeur peut notamment collecter et traiter les données personnelles suivantes vous concernant dans le but de se conformer à une exigence légale que le groupe Eurofeu doit respecter en tant qu'employeur : n° de sécurité sociale, relevé bancaire, carte d'identité, titre de séjour (si pertinent), notification d'accident ou maladie professionnelle, permis de conduire ou habilitation spécifique.

Confidentialité et informations sur les traitements de vos données personnelles : L'ensemble des données seront traitées de manière confidentielle et seront utilisées pour les nécessités de la gestion de l'entreprise, notamment l'administration du personnel. Vos données personnelles ne seront divulguées à des tiers que si vous avez donné votre consentement ou si l'Employeur est autorisé à divulguer ces informations en vertu de la loi applicable.

Vos données personnelles seront stockées par l'Employeur et pourront être le cas échéant utilisées par d'autres entités du groupe Eurofeu (notamment la société AER Holding) si nécessité de gestion de votre contrat de travail.

Le transfert de données entre sociétés du groupe Eurofeu sera réalisé conformément au Règlement Européen sur la protection des données personnelles.

L'Employeur peut engager des fournisseurs de services tiers qui auront accès à vos données personnelles et les traiteront ; étant précisé qu'aucun transfert de vos données personnelles ne sera opéré en dehors de l'UE, garantissant ainsi leur protection par le biais de la réglementation européenne désormais en vigueur.

L'Employeur peut conserver vos données personnelles pendant une durée de 5 années après la fin de votre contrat de travail, excepté les cas où la loi en dispose autrement.

Vos droits : Vous pouvez obtenir des informations supplémentaires sur les données personnelles conservées et traitées par l'Employeur vous concernant en contactant le Responsable des Données Personnelles à l'adresse suivante : dpo@eurofeu.fr ou par courrier RAR à l'adresse : DPO Groupe Eurofeu, 12 rue Albert Rémy, 28250 Senonches. Vous pouvez en outre vous opposer au traitement de vos données personnelles ou révoquer votre accord donné à ce traitement à tout moment. Si vous souhaitez révoquer votre accord, merci de contacter le DPO en lui indiquant votre demande. Si vous avez des réclamations d'une autre nature relativement au traitement de vos données personnelles par l'Employeur, vous pouvez également contacter la Commission Nationale Informatique et Liberté.

Article 19. Charte des réseaux sociaux : Le guide des bonnes pratiques sur les médias sociaux

Même dans le cadre d'une utilisation personnelle, nous devons respecter quelques règles de bonne conduite. Par exemple, sur votre profil professionnel (ou personnel mentionnant que vous êtes un salarié du Groupe Eurofeu) il faut bannir :

LES SUJETS SENSIBLES :

- La politique
- La religion

TOUT PROPOS :

- Injurieux
- Racistes
- Xénophobes
- Dégradants
- Insultants
- Provocateurs
- Harcèlement
- Insultes
- Diffamatoires sur l'entreprise
- Diffamatoires sur les collègues

Une limite à vos posts : Aucun chiffre ne doit être donné, la quantité d'appareils ou le chiffre d'affaires par exemple. Nous attirons votre attention sur le fait de faire attention aux photos que vous publiez. Elles doivent refléter une image professionnelle sans erreurs et incohérences techniques, mais aussi montrer une attitude et un comportement correct. Vous devez refléter une image d'un collaborateur qui respecte les règles de sécurité selon les règles communiquées par le Groupe. Exemple : bien porter ses EPI, respecter les gestes barrières et le port du masque lors d'une crise sanitaire. Gardez toujours un œil technique critique sur tous les détails.

Valoriser le Groupe : Il va de soi qu'il ne faut pas mettre en valeurs la concurrence en likant ou partageant leur poste. Cela implique techniquement du trafic sur les réseaux du concurrent et donc un manque à gagner pour nous. Si vous souhaitez valoriser des publications, valorisez celles du Groupe Eurofeu, c'est une question de bon sens.

Pas de dévalorisation de la concurrence : Critiquer les concurrents est déplacé et ne donne absolument pas une bonne image ni du Groupe ni de la personne qui écrit, même si les remarques sont vraies. En cas de difficulté à répondre à une attaque sur nos produits ou sur le Groupe, nous vous invitons à contacter le Service Marketing et Communication afin de vous aider à répondre, voire répondre au nom du Groupe. N'allez pas trop loin dans certains échanges qui pourraient s'avérer dangereux.

Plus d'informations : Vous n'êtes pas sûr de savoir si les informations professionnelles en votre possession sont confidentielles ? Demandez-vous si le fait de les partager sur internet pourrait nuire à l'entreprise et, dans le doute, parlez-en à votre Manager, ou à votre service Marketing. Vous avez une question, une remarque... N'hésitez pas à contacter l'équipe Marketing digital en écrivant à l'adresse e-mail suivante : cbouilly@eurofeu.fr

Charte relative au droit d'alerte professionnelle

Préambule

La loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, dite « loi Sapin 2 » a introduit au sein de la législation française le statut du lanceur d'alerte.

Le décret n° 2017-564 du 19 avril 2017 précise les conditions et modalités de la procédure qui doivent être mis en place.

La société ISOGARD, dont le siège est situé 12 Rue Albert Rémy - 28250 SENONCHES, représentée par Monsieur Éric HENTGES, en qualité de Directeur Général, établit la présente charte qui a pour objet de définir les dispositions particulières relatives aux modalités :

- de formulation et de recueil des signalements des lanceurs d'alerte
- de traitement des alertes

en précisant notamment le cadre légal.

Cette charte traduit la volonté de la Direction de la société ISOGARD de rendre la procédure accessible à l'ensemble des salariés de l'entreprise, ses collaborateurs occasionnels ou extérieurs.

Chapitre 1 – Définition

Article 1 – Champ d'application

Les dispositions de la présente charte s'appliquent aux mandataires sociaux et salariés de la société, ainsi qu'à ses collaborateurs extérieurs et occasionnels (intérimaires, stagiaires, prestataires de service), (ci-après désignés ensemble « les Collaborateurs »).

Article 2 – Définition du lanceur d’alerte et des faits susceptibles de faire l’objet d’une alerte

Le lanceur d’alerte est une personne physique qui révèle ou signale, de manière désintéressée et de bonne foi :

- une violation grave et manifeste d’un engagement international régulièrement ratifié ou approuvé par la France, d’un acte unilatéral d’une organisation internationale pris sur le fondement d’un tel engagement, de la loi ou du règlement,
- une menace ou un préjudice grave pour l’intérêt général,
- un crime ou un délit,

dont elle a eu personnellement connaissance.

Le lanceur d’alerte peut être un salarié, mais également un collaborateur occasionnel tel qu’un stagiaire ou même un collaborateur extérieur tel qu’un consultant, un intermédiaire, un sous-traitant ou un fournisseur. Il ne peut jamais s’agir d’une personne totalement tierce à l’entreprise sans aucun lien contractuel que ce soit dans le cadre d’un contrat de travail ou d’un contrat de prestation de service.

Les faits peuvent par exemple être une fraude, une corruption, une pratique anticoncurrentielle déloyale, une mise en danger de la vie d’autrui (en termes de santé ou sécurité), un fait de discrimination ou de harcèlement, une mise en danger de l’environnement, etc.

Les faits, informations ou documents, quel que soit leur forme ou leur support, couvert par le secret de la défense nationale, le secret médical ou le secret des relations entre un avocat et son client sont exclus du régime d’alerte.

Article 3 – Politique d’entreprise

ISOGARD s’engage pour la protection des lanceurs d’alerte dans le respect de la loi française. ISOGARD a notamment pour objectif d’accompagner la démarche et les moyens d’expression de ses Collaborateurs, afin que chacun puisse être un acteur de l’éthique et de la prévention des risques de la société.

Article 4 – Caractère complémentaire

ISOGARD confère au droit d’alerte un dispositif complémentaire offert aux salariés. Il n’a pas vocation à se substituer aux autres canaux d’alerte de communication interne existants en application des règles en vigueur, notamment la voie hiérarchique, ou par l’intermédiaire des représentants du personnel ou des audits internes.

Le dispositif est mis en place pour permettre aux Collaborateurs de signaler un fait lorsque les modes normaux d’alerte ne peuvent pas fonctionner ou ne sont pas considérés comme adaptés.

Article 5 – Garantie de confidentialité et catégorie de données traitées

Le dispositif d'alerte garantit la confidentialité et le respect des droits de chacun dans le traitement des démarches engagées.

La procédure de recueil des signalements instituée par la présente charte garantit la stricte confidentialité de l'identité :

- du lanceur d'alerte ;
- des personnes visées par le lanceur d'alerte (principe de la présomption d'innocence);
- des informations recueillies par l'ensemble des destinataires du signalement.

Les faits recueillis sont strictement limités aux actes visés par le dispositif d'alerte et seules les données liées à ces faits pourront être collectées et traitées. Ces informations concernent les données suivantes :

- identité, fonctions et coordonnées de l'émetteur de l'alerte professionnelle ;
- identité, fonctions et coordonnées des personnes faisant l'objet d'une alerte ;
- identité, fonctions et coordonnées des personnes intervenant dans le recueil ou dans le traitement de l'alerte ;
- faits signalés ;
- éléments recueillis dans le cadre de la vérification des faits signalés ;
- compte rendu des opérations de vérification ;
- suites données à l'alerte.

La prise en compte de l'alerte professionnelle ne s'appuie que sur des données formulées de manière objective, en rapport direct avec le périmètre du dispositif d'alerte et strictement nécessaires à la vérification des faits allégués. Les formulations utilisées pour décrire la nature des faits signalés feront apparaître leur caractère présumé.

La stricte confidentialité de l'auteur du signalement, des faits faisant l'objet du signalement et des personnes visées, ainsi que des échanges entre le lanceur d'alerte et du référent sera garantie et sécurisée, y compris en cas de communication à des tiers dès lors que celle-ci est nécessaire pour les seuls besoins de la vérification ou du traitement du signalement.

Toute donnée ne rentrant pas ou plus dans le champ du dispositif ne sera pas traitée dans le cadre de la présente procédure, et sa destruction ou sa conservation sera assurée dans les conditions de l'article 15 ci-dessous.

En outre, les éléments de nature à identifier :

- le lanceur d'alerte ne peuvent être divulgués, sauf à l'autorité judiciaire, qu'avec le consentement de celui-ci ;
- la personne mise en cause par un signalement ne peut être divulgués, sauf à l'autorité judiciaire, qu'une fois le caractère fondé de l'alerte établi.

Les personnes ayant recueilli et / ou traité un signalement émis par un lanceur d'alerte sont tenus d'observer cette obligation de confidentialité.

Cette obligation ne concerne pas les personnes initialement destinataires d'un signalement par un lanceur d'alerte, lorsqu'elles transmettent ce signalement au Référent.

Article 6 – Protection du lanceur d’alerte

Il est rappelé que, conformément à l’article 122-9 du code pénal, n’est pas pénalement responsable la personne qui porte atteinte à un secret protégé par la loi, dès lors que cette divulgation est nécessaire et proportionnée à la sauvegarde des intérêts en cause, qu’elle intervient dans le respect des procédures de signalement définies par la loi et que la personne répond aux critères de définition du lanceur d’alerte prévus à l’article 6 de la loi n° 2016-1691 du 9 décembre 2016.

En outre, aux termes de l’article L. 1132-3-3 du code du travail, aucune personne ne peut être écartée d’une procédure de recrutement ou de l’accès à un stage ou à une période de formation professionnelle, aucun salarié ne peut être sanctionné, licencié ou faire l’objet d’une mesure discriminatoire, directe ou indirecte, notamment en matière de rémunération, au sens de l’article L. 3221-3, de mesures d’intéressement ou de distribution d’actions, de formation, de reclassement, d’affectation, de qualification, de classification, de promotion professionnelle, de mutation ou de renouvellement de contrat, pour avoir signalé une alerte dans le respect des articles 6 à 8 de la loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique.

Compte tenu de ces éléments, et sous réserve de l’appréciation souveraine des juges, la personne qui émet un signalement en dehors des conditions prévues par les textes en vigueur, ainsi que la présente charte ne pourra pas bénéficier du statut du lanceur d’alerte et des garanties associées.

Article 7 – Caractère facultatif, sanctions, représailles

L’usage du dispositif d’alerte professionnelle par les Collaborateurs est facultatif et sa non-utilisation n’entraîne aucune conséquence pour eux. Aucune sanction ne pourra ainsi être prise à l’encontre d’un Collaborateur au motif que ce dernier n’aurait pas fait usage de ce dispositif d’alerte.

Tout Collaborateur qui, sciemment, ou de manière manifestement négligente, ferait de fausses déclarations en pleine connaissance de cause, divulguerait des informations trompeuses, agirait de mauvaise foi ou de manière abusive, sera susceptible de faire l’objet de mesures disciplinaires ou de poursuites conformément aux lois et réglementations applicables.

A l’inverse, conformément aux dispositions de l’article L.1132-3 du code du travail, l’utilisation de bonne foi du dispositif, même si les faits reportés s’avèrent par la suite inexacts ou ne donnent lieu à aucune suite, n’exposera son auteur à aucune sanction disciplinaire. Les mesures nécessaires et raisonnables seront prises afin de le protéger si l’alerte est effectuée de bonne foi dans le cadre de la présente procédure, notamment contre toutes représailles, critiques ou poursuites disciplinaires.

Aucun Collaborateur ne saurait non plus faire l’objet de harcèlement, ou subir des conséquences négatives quant à son emploi pour avoir émis une alerte de bonne foi.

Chapitre 2 – Formulation et recueil des signalements d'alerte

Article 8 – Destinataire du signalement et référent

Le Collaborateur porte le signalement à la connaissance :

- de son supérieur hiérarchique direct ou indirect ;
- ou du Directeur Général Adjoint ;
- ou du Référent identifié par le présent accord.

Il est procédé à la désignation d'un Référent ayant pour missions de réceptionner les alertes et d'assurer leur traitement (ci-après le « Référent »).

Il a été décidé d'attribuer ces missions à : Baptiste COCHIN, Juriste Groupe & DPO.

Les coordonnées du Référent sont les suivantes : alerte@eurofeu.fr ; Tél. : 02.37.53.57.93.

Le Collaborateur porte son signalement à l'attention de la personne précédemment visée selon l'un des moyens suivants :

- courrier électronique à l'adresse e-mail du Référent ci-dessus ;
- ou courrier recommandé avec accusé de réception à l'adresse suivante : ISOGARD, 12 Rue Albert Rémy - 28250 SENONCHES

Autant que faire se peut, afin de garantir la confidentialité prévue par le présent accord, le signalement communiqué par courrier recommandé est transmis sous double enveloppe. Tous les éléments relatifs au signalement sont insérés dans une première enveloppe fermée (dite enveloppe intérieure). Sur cette enveloppe, figure exclusivement la mention « signalement d'une alerte ».

L'enveloppe est ensuite insérée dans une enveloppe extérieure sur laquelle figure le nom et les coordonnées de la personne destinataire du signalement.

Les courriers électroniques devront comporter en objet la mention « signalement d'une alerte ».

Article 9 – Contenu du signalement

Le signalement est :

- écrit et comporte de manière précise et détaillée les faits qui font l'objet du signalement ;
- accompagné de tous les éléments quel que soit leur forme ou leur support de nature à l'étayer et à faciliter son traitement.

Le lanceur d'alerte fournit également ses coordonnées afin qu'il puisse, le cas échéant, être contacté par le Référent.

Ces éléments sont transmis dans les mêmes formes que le signalement.

Si une personne souhaite rester anonyme, le signalement ne sera traité que si la gravité des faits mentionnés est établie et que les éléments factuels sont suffisamment détaillés. En outre, il sera procédé à un examen approfondi de son contenu avant d'initier la procédure prévue par la présente charte pour les alertes.

Il est précisé que les éléments de nature à identifier l'émetteur de l'alerte ne peuvent être divulgués, sauf à l'autorité judiciaire, qu'avec le consentement de la personne. Les éléments de nature à identifier la personne mise en cause par un signalement ne peuvent être divulgués, sauf à l'autorité judiciaire, qu'une fois établi le caractère fondé de l'alerte.

Chapitre 3 – Traitement de l'alerte

Article 10 – Centralisation auprès du Référent

Quelle que soit la personne auprès de laquelle est porté le signalement, il appartient à cette dernière de transmettre, sans délai, celui-ci au Référent qui est seul compétent pour traiter l'alerte. Sont ainsi transmis l'identité du lanceur d'alerte et le contenu du signalement. Le lanceur d'alerte est informé de cette transmission.

La transmission du signalement au Référent ne délie pas la personne initialement informée de la confidentialité qu'elle doit observer en application des articles 5 et 16 de la présente charte à l'exception de l'information obligatoire du Référent.

Article 11 – Information transmise au lanceur d'alerte

Dès que le Référent a pris connaissance du signalement, il informe sans délai le lanceur d'alerte

- de la réception du signalement ;
- du délai dont il dispose pour procéder à l'examen du signalement ;
- de la durée prévisible de l'examen compte tenu des éléments communiqués ;
- des modalités selon lesquelles le lanceur d'alerte sera informé des suites données au signalement.

Cette information est portée à la connaissance du lanceur d'alerte selon l'un des moyens suivants :

- courrier remis en main propre contre signature ;
- courrier recommandé ;
- courrier électronique.

Le Référent disposera des moyens nécessaires pour procéder à toute enquête (dont entretien avec les personnes concernées) qu'il juge opportune.

Article 12 – Délai de traitement de l'alerte

Le Référent doit vérifier la recevabilité du signalement dans un délai raisonnable dépendant de la complexité de l'alerte qui lui est soumise. Le Collaborateur est informé de la suite donnée à celle-ci.

En l'absence d'information au terme de ce délai, le lanceur d'alerte peut communiquer son signalement à l'autorité judiciaire, à l'autorité administrative ou aux ordres professionnels compétents.

En dernier ressort, à défaut de traitement dans un délai de trois mois, le signalement peut être rendu public.

Article 13 – Information transmise à la personne visée par l'alerte

La personne qui fait l'objet d'une alerte est informée par le Référent dès l'enregistrement, informatisé ou non, de données la concernant afin de lui permettre de s'opposer au traitement de ces données.

Lorsque des mesures conservatoires sont nécessaires, notamment pour prévenir la destruction de preuves relatives à l'alerte, l'information de cette personne intervient après l'adoption de ces mesures.

Cette information est réalisée par :

- courrier remis en main propre contre signature ;
- courrier recommandé ;
- courrier électronique.

Elle précise notamment :

- le responsable du dispositif ;
- les faits reprochés ;
- les personnes destinataires de l'alerte ;
- les modalités d'exercice des droits d'accès et de rectification.

Article 14 – Suite de l'alerte

Le lanceur d'alerte est informé de la suite donnée à son signalement par :

- courrier remis en main propre contre signature ;
- courrier recommandé ;
- courrier électronique.

S'il est estimé qu'il ne doit pas être donné de suite à l'alerte, le lanceur d'alerte et les personnes visées par le signalement sont informées de la clôture de la procédure par :

- courrier remis en main propre contre signature ;
- courrier recommandé ;
- courrier électronique.

Article 15 – Conservation et durée de conservation des données à caractère personnel

Les données relatives à une alerte considérée, dès son recueil par le responsable du traitement, comme n'entrant pas dans le champ du dispositif sont détruites ou archivées sans délai, après anonymisation.

Lorsque l'alerte n'est pas suivie d'une procédure disciplinaire ou judiciaire, les données relatives à cette alerte sont détruites ou archivées, après anonymisation, par l'organisation chargée de la gestion des alertes dans un délai de deux mois à compter de la clôture des opérations de vérification.

Lorsqu'une procédure disciplinaire ou des poursuites judiciaires sont engagées à l'encontre de la personne mise en cause ou de l'auteur d'une alerte abusive, les données relatives à l'alerte sont conservées par l'organisation chargée de la gestion des alertes jusqu'au terme de la procédure.

Les données faisant l'objet de mesures d'archivage sont conservées, dans le cadre d'un système d'information distinct à accès restreint, pour une durée n'excédant pas les délais de procédures contentieuses.

CHAPITRE 4 – Conditions générales

Article 16 – Information des utilisateurs potentiels du dispositif

La présente charte est diffusée sur le portail intranet de la société et mentionnée sur les panneaux d'affichage de la société.

Elle est également mise à disposition au service Ressources Humaines de l'entreprise.

Article 17 – Entrée en vigueur - Durée de la charte

La présente charte entre en application le 10 mai 2023 et est conclue pour une durée indéterminée.

Article 18 – Révision – Dénonciation

La présente charte pourra être dénoncée, à tout moment en respectant le délai de préavis de 3 mois.

Article 19 – Règles de publicité

La présente charte a été soumise à l'avis du Comité Social et Économique en date du 22 février 2023.

La présente charte fera l'objet d'un dépôt, à savoir :

- en deux exemplaires auprès de l'inspecteur du travail. Ce dépôt sera accompagné de l'avis du Comité Social et Économique ;
- en un exemplaire auprès du greffe du conseil de prud'hommes de Dreux.

Faits à Senonches, le 22 février 2023

Pour la Direction

Monsieur Éric HENTGES
Directeur Général

A handwritten signature in black ink, appearing to be 'Eric Hentges', written in a cursive style.

CODE DE CONDUITE

**Règles anticorruptions du groupe eurofeu
annexées au Règlement intérieur**



Eurofeu Company SAS
SAS au capital de 30.628.763 €
884 194 945 RCS Chartres
NAF 6630Z - TVA FR 52 884194945
Siège social : 12 rue Albert Rémy
28250 Senonches - France

Préambule

La commission d'un acte de corruption ou de trafic d'influence est un acte grave et illégal, qui peut entraîner des conséquences importantes pour celui qui commet l'acte mais également pour le groupe Eurofeu, ainsi que pour ses filiales françaises et étrangères (le « Groupe Eurofeu » ou le « Groupe »), le cas échéant.

Conformément à l'article 17 de la loi Sapin II¹, un dispositif spécifique de lutte contre la corruption, notamment au travers d'une cartographie des risques, un dispositif de formation des personnels les plus exposés, et un dispositif de contrôle interne adapté sont en cours de déploiement.

Le présent Code de conduite anticorruption (ci-après le « Code ») est une étape supplémentaire dans la démarche engagée à ce titre. Il est intégré au règlement intérieur des sociétés du Groupe.

Plus particulièrement, ce Code a pour objet de rappeler à tous, les principes de base relatifs à la lutte contre la corruption et le trafic d'influence et a ainsi vocation à identifier, au sein du Groupe Eurofeu, les situations à risque et les règles de conduite à adopter à cet égard.

Il s'applique à l'ensemble des dirigeants, mandataires sociaux et personnels permanents (collaborateurs en CDI) et occasionnels (stagiaires, CDD, contrats de professionnalisation, travailleurs intérimaires, prestataires sur site) du Groupe Eurofeu, (ci-après les « Collaborateurs »).

Il est également attendu de l'ensemble de nos partenaires commerciaux (prestataires, intermédiaires, fournisseurs, clients, etc.) qu'ils se conforment aux principes du présent Code ou qu'ils appliquent des standards au moins équivalents à celui-ci.

Ce Code ne prétend pas être exhaustif et n'a pas vocation à couvrir toutes les situations auxquelles les Collaborateurs pourraient être confrontés. Il expose les règles qui doivent gouverner leurs décisions.

A ce titre, les dirigeants du Groupe Eurofeu ont un devoir d'exemplarité et doivent promouvoir une conduite éthique des affaires dans le respect des dispositions du présent Code.

L'encadrement veille également à ce que ces règles de conduite soient appliquées au sein de leurs équipes et est à l'écoute des préoccupations éthiques de ses collaborateurs.

Il appartient donc à chacun de lire attentivement et de comprendre les règles exposées dans ce Code et de faire preuve de discernement et de bon sens face aux diverses situations qui peuvent se présenter.

Eric HENTGÈS
Président

¹ Loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique.

Focus : Le coût de la corruption dans le monde et en Europe

Quelle que soit sa forme, la corruption entraîne des conséquences économiques et sociales graves et contribue à l'instabilité et à la pauvreté dans le monde. Elle constitue un facteur dominant de conduite vers l'échec des pays fragiles, souligne l'ONU². La nature et les impacts de la corruption dans le monde sont difficilement quantifiables, mais certaines ONG ou organisations internationales comme le FMI ont donné un aperçu du phénomène. Voici leurs conclusions, en trois chiffres³.

1500 à 2000 milliards de dollars : C'est le coût des pots-de-vin versés chaque année dans le monde selon le FMI⁴. Cela représente près de 2% du PIB mondial. Et il ne s'agit là que de l'un des aspects de la corruption ! Les détournements de fonds publics représenteraient quelque 2600 milliards de dollars, soit plus de 5% du PIB mondial. Selon l'ONU, la corruption entraîne moins de prospérité, moins de respect des droits, moins de services et moins, moins d'emplois...

Entre 179 et 990 milliards d'euros : Cette large fourchette est celle du coût annuel de la corruption au sein de l'Union européenne. Le scénario le plus optimiste l'évalue entre 179 et 256 milliards, le plus pessimiste le situe à 990 milliards, soit 6,3% du PIB européen⁵. Le coût de la corruption sur les marchés publics est, lui, évalué à 5 milliards d'euros par an : la France se place à la 5^e place des pays européens les plus touchés.

23 : C'est la place de la France dans le classement mondial de la corruption en 2020, publié par Transparency international⁶. Au total, 179 pays figurent dans ce classement établi à partir d'un « indice de perception de la corruption » qui note les pays de 0 (pays perçu comme très corrompu) à 100 (pays perçu comme très peu corrompu). En 2020, la France a obtenu la note de 69, très loin du trio de tête formé par le Danemark (88), la Nouvelle-Zélande (88) et la Finlande (85). Globalement, Transparency fait un constat alarmant : « dans le monde entier, la corruption systémique et l'inégalité sociale se renforcent mutuellement, conduisant à une désillusion populaire vis-à-vis du monde politique et fournissant un terreau fertile à la montée des politiciens populistes ».

² <http://www anticorruptionday.org/>

³ <https://www.lefigaro.fr/conjoncture/2017/12/09/20002-20171209ARTFIG00019-trois-chiffres-edifiants-demonstrent-que-la-corruption-gangrene-le-monde.php>

⁴ <https://www.imf.org/fr/News/Articles/2017/09/18/sp091817-addressing-corruption-with-clarity>

⁵ Étude publiée en 2016 par le Parlement européen, portant à la fois sur les coûts directs et indirects de la corruption dans les 28 États membres.

⁶ <https://www.transparency.org/en/cpi/2020/index/nzl#>

Qu'est-ce que la corruption et le trafic d'influence ?

Sous le terme générique de « corruption » sont visés la corruption proprement dite et le trafic d'influence.

La corruption est un délit qui se développe dans les « zones grises » du business, notamment dans les échanges avec les tiers (fournisseurs, prestataires, intermédiaires, partenaires, etc.).

La **corruption** proprement dite est le fait de solliciter ou d'accepter directement ou indirectement des offres, des promesses, des dons, des présents ou des avantages quelconques pour soi-même ou pour autrui pour accomplir ou avoir accompli, ou s'abstenir d'accomplir un acte de sa fonction, de sa mission ou l'avoir facilité par sa fonction, sa mission⁷.

Le **trafic d'influence** est caractérisé lorsqu'un don ou un avantage indu est offert ou consenti pour que le bénéficiaire use de son influence, réelle ou supposée, en vue d'obtenir d'une autorité publique une décision favorable⁸.

Le point commun de la corruption et du trafic d'influence est le dévoiement de la fonction exercée par le bénéficiaire de l'avantage indu (la personne corrompue) qui monnaye le pouvoir ou l'influence que lui procure sa fonction, dans son intérêt personnel, direct ou indirect.

Il existe deux types de corruption :

La corruption est active, lorsque c'est la personne qui corrompt qui est à l'initiative de la corruption (« le corrupteur ») en proposant ou fournissant une somme d'argent ou toute autre contrepartie ou avantage en échange d'un service.

La corruption est passive, lorsque l'acte de corruption est à l'initiative de la personne qui est corrompue (« le corrompu »), en exigeant ou acceptant de l'argent ou tout autre avantage en échange d'un service.

Enfin, la corruption est dite **publique** lorsqu'elle implique des personnes exerçant une fonction publique (ci-après « Agent public »⁹) et **privée** lorsque l'infraction de corruption n'implique que des personnes physiques ou morales relevant du secteur privé.

⁷ Conformément aux articles 432-11, 433-1 et 433-25 du code pénal, la commission du délit de corruption peut donner lieu aux sanctions suivantes :

- Personne physique : 5 à 10 ans d'emprisonnement et 500 000 à 1 000 000 euros d'amende ou doublement du produit de l'infraction ;
- Personne morale : 2 500 000 à 5 000 000 euros ou doublement du produit de l'infraction, plus des peines complémentaires.

Conformément aux articles susvisés, la commission du délit de trafic d'influence donne lieu aux mêmes sanctions que celles prévues en cas de commission du délit de corruption. La notion d'agent public doit être interprétée largement et vise toute personne dépositaire de l'autorité publique, chargée d'une mission de service public ou investie d'un mandat électif public, pour elle-même ou pour autrui. Doit être également qualifié d'Agent public, toute autre personne considérée comme tel en vertu de la législation nationale d'un pays.

⁸ Conformément aux articles susvisés, la commission du délit de trafic d'influence donne lieu aux mêmes sanctions que celles prévues en cas de commission du délit de corruption.

⁹ La notion d'agent public doit être interprétée largement et vise toute personne dépositaire de l'autorité publique, chargée d'une mission de service public ou investie d'un mandat électif public, pour elle-même ou pour autrui. Doit être également qualifié d'Agent public, toute autre personne considérée comme tel en vertu de la législation nationale d'un pays.

C'est ainsi que les exemples de corruption sont nombreux :

- ➔ Versement d'un « dessous de table » ou d'un « pot de vin » à une personne décisionnaire pour qu'elle intervienne de manière favorable au bénéfice de son interlocuteur.
- ➔ Octroi d'une invitation privilégiée à un Agent public dans l'attente d'une contrepartie.
- ➔ Rémunération d'un intermédiaire pour que celui-ci use de son influence auprès d'une municipalité afin de favoriser la conclusion d'un marché.

Les actions du Groupe Eurofeu doivent ainsi être conformes aux principes et règles internes du groupe et ne jamais servir à avantager indûment, influencer abusivement ou même donner l'apparence d'influencer abusivement quelque décisionnaire que ce soit.

Les règles à respecter

Le présent chapitre fournit les informations nécessaires pour comprendre et mettre en œuvre les règles à respecter par les Collaborateurs dans le cadre de leurs activités afin de prévenir et de lutter contre la corruption.

Cadeaux et invitations

Offrir ou accepter des cadeaux et invitations est souvent considéré comme un acte de courtoisie permettant de renforcer les relations commerciales. Cependant, les règles en matière de lutte contre la corruption interdisent l'offre de cadeaux, invitations et autre à un tiers dans le but d'obtenir un avantage indu ou d'exercer de façon non justifiée une quelconque influence sur toute action officielle.

Ainsi, l'offre ou l'acceptation de cadeaux ou invitations peut être considérée comme l'une des formes manifestes de corruption, notamment dans le cadre d'une opération commerciale ou d'une demande d'autorisation/permis auprès d'un Agent public.

Les règles à respecter :

- Les Collaborateurs doivent communiquer à leurs partenaires commerciaux les règles du Groupe Eurofeu relatives aux cadeaux et invitations et s'enquérir des leurs.
- Les cadeaux et invitations doivent être d'une valeur raisonnable, adaptés aux circonstances et correspondre aux usages commerciaux (ex : cadeau de fin d'année, repas de fin de mission, etc.).
- Plus particulièrement, l'acceptation et l'offre de **cadeaux** sont tolérées s'ils sont d'une valeur inférieure à **150 € TTC** par personne, par an et par partenaire commercial. Au-delà de ce seuil, l'acceptation ou l'offre de cadeaux par un Collaborateur est soumise à **l'autorisation préalable de son responsable hiérarchique**.
- **Les cadeaux en espèces ou équivalents tels que les bons ou chèques cadeaux sont interdits.**
- Les cadeaux et invitations ne peuvent être reçus ou offerts que s'ils ne sont pas interdits par la loi. Lorsqu'ils sont autorisés, offrir ou accepter un cadeau ou une invitation doit rester exceptionnel.
- Dans tous les cas, les cadeaux et invitations offerts ou reçus de la part d'un Agent public sont interdits.
- Les cadeaux et invitations se font dans un cadre strictement professionnel. Ils ne peuvent être reçus au domicile du Collaborateur et ne peuvent concerner que le Collaborateur ou le partenaire commercial, à l'exclusion de la famille ou autres relations de ceux-ci.

En cas d'absence de validation, le cadeau reçu devra, sur décision hiérarchique, être renvoyé au partenaire commercial, accompagné d'un courrier de remerciement rappelant les règles du Groupe Eurofeu en matière d'acceptation de cadeaux.

- ➔ Les Collaborateurs doivent, dans la mesure du possible, partager le cadeau reçu au sein de leur équipe (ex : bien consommable tel qu'une boîte de chocolat) ou procéder à un tirage au sort.
- ➔ L'acceptation et l'offre par un Collaborateur d'**invitations** (repas d'affaire, événement professionnel, etc.) sont tolérées uniquement si celles-ci sont liées à l'activité normale du Collaborateur, sont en lien avec les projets et activités du Groupe, et si leur valeur estimée est inférieure à **150 € TTC**.
- ➔ L'acceptation et l'offre d'invitations supérieures à 150 € TTC, de nature plus exceptionnelle (spectacles, événements sportifs, etc.), et/ou hors temps de travail (week-end, congés, jours fériés), doivent impérativement faire l'objet d'une **demande préalable d'autorisation au responsable hiérarchique**.
- ➔ Le Collaborateur ne peut accepter une invitation à un événement que si le partenaire commercial qui invite est présent lors de l'événement.
- ➔ Les cadeaux et invitations doivent se dérouler à distance de toute prise de décision importante (procédure de mise en concurrence, appel d'offres, etc.). En effet, les circonstances du cadeau ou de l'invitation ne doivent pas être de nature à inspirer des soupçons de corruption, même a posteriori. Il faut donc être attentif au contexte et au sens que peut prendre un avantage ou un cadeau qui ne doit supposer aucune attente en contrepartie.

Si les conditions ci-dessus ne sont pas respectées, le cadeau ou l'invitation doit être immédiatement restitué par le Collaborateur, accompagné d'un courrier de remerciement rappelant les règles du Groupe Eurofeu en matière d'acceptation de cadeaux et invitations.

En tout état de cause, si la législation locale est plus stricte que les règles ci-dessus énoncées, il convient de se conformer à la règle la plus stricte.

Partenaires commerciaux

Le risque de corruption existe dès lors que le Groupe Eurofeu est en relations d'affaires avec différents partenaires commerciaux dans le cadre de ses activités professionnelles (« Business to Business »).

En effet, dans certaines circonstances, une entreprise peut être tenue juridiquement responsable pour des faits de corruption commis par son partenaire commercial. Les partenaires commerciaux du Groupe Eurofeu sont notamment des :

- Fournisseurs ;
- Sous-traitants ;
- Intermédiaires ;
- Distributeurs de produits de sécurité incendie ;
- Conseils (consultants, banques, avocats, etc.) ;
- Clients.

Les règles à respecter :

- ➔ Avant d'entrer en relation d'affaires avec un fournisseur, sous-traitant ou intermédiaire, il convient d'effectuer des contrôles préalables afférents à son intégrité (« due diligences ») adaptés et proportionnés à la situation particulière du partenaire commercial, conformément aux procédures internes (questionnaire d'évaluation « Fournisseur » à remplir avec le Service Achats).
- ➔ Penser chaque action dans l'intérêt des clients et des réseaux de distribution et dans le respect des lois et règlements ; être à l'écoute et connaître au mieux les besoins des clients, pour leur fournir des conseils et un accompagnement adapté ; fournir aux clients et aux distributeurs une information claire, exacte et non trompeuse ; faire remonter au manager tout dysfonctionnement et toute situation pouvant entraîner un conflit d'intérêt.
- ➔ Tout recours à un partenaire commercial doit donner lieu à l'établissement d'un contrat écrit. Ces contrats doivent explicitement contenir des clauses certifiant que le co-contractant se conforme aux règles et lois luttant contre la corruption, et prévoir la nullité du contrat en cas de violation de ces règles.
- ➔ Les règlements effectués au bénéfice d'un partenaire commercial doivent toujours correspondre à une rémunération appropriée et proportionnée au service rendu. Il convient d'être particulièrement vigilant sur les règlements effectués sur un compte bancaire domicilié à l'étranger.
- ➔ Aucun paiement ne doit être effectué en espèces ou sans un accord contractuel dûment approuvé.
- ➔ Ces paiements doivent être effectués après présentation d'une facture, dûment validée, en priorité par virement bancaire sur le compte bancaire du partenaire commercial, après vérification des coordonnées bancaires du bénéficiaire, et pour le montant figurant sur la facture, conformément aux dispositions contractuelles. En outre, ils doivent être consignés dans les comptes de la société.
- ➔ **Les paiements par chèque doivent demeurer exceptionnels et justifiés par l'impossibilité de faire un virement bancaire.**
- ➔ Il convient de vérifier la réalité de la prestation délivrée et réaliser un rapprochement entre les conditions financières figurant dans le contrat et les factures réglées.

Concurrence

Le droit de la concurrence est constitué d'un ensemble de règles applicables aux entreprises qu'elles soient privées ou publiques qui opèrent sur différents marchés. Il a pour but de maintenir le principe d'une concurrence libre et loyale. De nombreux comportements peuvent entraver le libre jeu de la concurrence comme les ententes, les abus de position dominante.

Une entente est un accord, une concertation ou une collaboration délibérée et intentionnelle entre entreprises ayant pour objet ou pour effet, même potentiel, de coordonner leur comportement, limitant ainsi la concurrence. Une entente avec une entreprise concurrente ou non, peut prendre la forme d'un accord oral, écrit, formel ou informel (repas d'affaires, rencontre dans des associations professionnelles...).

Au-delà des formes les plus graves d'entente que sont les cartels - la fixation en commun des prix de vente ou de conditions commerciales -, la répartition de clientèles ou de marchés, la coordination d'appels d'offres ou encore la décision conjointe de boycotter un client ou un fournisseur, constituent également une entente.

L'abus de position dominante vise une entreprise qui se trouve dans la position d'agir unilatéralement, sur un marché donné : politique de prix visant à l'élimination des concurrents ou stratégie commerciale d'éviction, pratiques discriminatoires... Sont considérées comme des informations sensibles des données non publiques utiles sur le plan stratégique (information sur les prix et leurs tendances d'évolution, liste des clients, capacité de marché et modes de distribution, stratégie, coûts...). Il est cependant possible d'échanger certaines informations avec les concurrents d'Eurofeu dès lors qu'elles sont publiques, relatives à un thème d'intérêt général pour la profession ou dans le cadre d'organisations professionnelles.

Les règles à respecter :

- ➔ Toutes les activités du groupe Eurofeu doivent être réalisées dans le respect du droit de la concurrence, dont le principe de base est que les entreprises opérant sur un marché doivent déterminer leur stratégie de façon autonome. Les ententes entre entreprises indépendantes ainsi que les abus de position dominante sont donc strictement interdites.
- ➔ En cas de doute sur le caractère sensible d'une information, effectuer une vérification auprès de mon responsable et du service juridique avant tout échange avec un concurrent ou une organisation professionnelle.
- ➔ Dans le cadre de relations formelles et obligées avec des concurrents, indiquer clairement l'objet de l'échange, limiter l'échange strictement à son objet et en garder une trace écrite ; contacter la Direction Juridique avant tout accord susceptible d'avoir un effet concurrentiel sensible sur le marché de la sécurité incendie.
- ➔ En aucun cas, nous ne devons discuter, nous mettre d'accord ou échanger des informations avec la concurrence (ou même simplement recevoir de telles informations de la concurrence) sur (i) les prix pratiqués par notre groupe ou ceux pratiqués par un concurrent avec ses clients, (ii) les niveaux de remise obtenus par notre groupe ou ceux obtenus par un concurrent, (iii) la stratégie de fixation de prix à venir ou (iv) les autres conditions (les remises de fin d'année par exemple) obtenues par le groupe. De telles informations ne doivent pas non plus être demandées à un concurrent.

Conflits d'intérêts

Le conflit d'intérêts désigne toute situation où les intérêts personnels d'un Collaborateur (ou ceux d'une personne morale ou physique à laquelle il est lié ou proche) sont contraires aux intérêts du Groupe Eurofeu.

Par intérêt personnel, il faut entendre les intérêts qui pourraient influencer ou paraître influencer sur la manière dont le Collaborateur s'acquitte des fonctions et responsabilités qui lui ont été confiées par le Groupe.

Une telle situation pourrait par exemple survenir si un Collaborateur :

- négocie au nom du Groupe Eurofeu un contrat dont il retire un intérêt personnel actuel ou ultérieur ;
- Détient un intérêt financier dans une société contrôlée par des concurrents ou encore des clients du Groupe Eurofeu, etc.

Dans la mesure où un conflit d'intérêts peut cacher un acte de corruption, il est primordial que les Collaborateurs soient vigilants quant à la survenance de situations de conflits d'intérêts.

Les règles à respecter :

- ➔ Les Collaborateurs doivent toujours privilégier les intérêts du Groupe Eurofeu en s'abstenant de mettre en avant tout intérêt personnel, financier ou familial.
- ➔ En cas de conflits d'intérêts potentiels ou avérés, les Collaborateurs doivent informer leur hiérarchie au plus vite et, à tout le moins, avant toute prise de décision concernant la relation d'affaires avec le partenaire commercial en question. Dans ce cas, les Collaborateurs doivent s'abstenir de participer au processus décisionnel.

Paielements de facilitation

Les paiements de facilitation constituent des sommes d'argent, souvent modestes, sollicitées par des Agents publics afin d'obtenir ou d'accélérer l'accomplissement de certains actes administratifs (traitement de documents étatiques, délivrance d'autorisations ou de permis, etc.). Ces paiements sont interdits dans la plupart des pays.

La règle à respecter :

- Le Groupe Eurofeu interdit les paiements de facilitation et ce, même dans l'hypothèse où les lois locales les autorisent.

Recrutement

Le recrutement d'un nouveau Collaborateur au sein du Groupe Eurofeu peut potentiellement donner lieu à un acte de corruption dans le cas où le Groupe se verrait octroyer par un tiers un avantage indu en contrepartie de l'embauche d'un candidat particulier ; notamment afin d'en tirer un bénéfice relatif à une future contractualisation ou une influence sur une décision administrative.

La règle à respecter :

- ➔ Tout avantage indu (personnel ou dans le cadre de ses fonctions) octroyé par un tiers en échange du recrutement d'un Collaborateur est interdit.
- ➔ Comme pour tout conflit d'intérêt, les Collaborateurs doivent toujours privilégier les intérêts du Groupe Eurofeu en s'abstenant de mettre en avant tout intérêt personnel, financier ou familial lors d'un recrutement. Le cas échéant, les Collaborateurs doivent informer leur hiérarchie au plus vite et, à tout le moins, avant toute prise de décision concernant ledit recrutement.

Lobbying

Le lobbying est toute activité destinée à intervenir auprès d'un gouvernement ou d'une institution en faveur d'une cause particulière ou d'un résultat attendu. Plus particulièrement, il s'agit d'une contribution constructive et transparente, à l'élaboration des politiques publiques sur les sujets pertinents liés aux activités d'un Groupe. Cette contribution vise à enrichir la réflexion des décideurs publics.

Le lobbying devient de la corruption dans le cas où la personne exerçant une activité de lobbying offrirait un avantage à un Agent public afin de l'inciter à soutenir une législation ou des activités qui lui seraient favorables.

Les règles à respecter :

- ➔ Faire preuve d'intégrité, de probité intellectuelle et de transparence dans toutes les relations avec les institutions et/ou Agents publics, et ce, quel que soit la situation ou l'intérêt défendu.
- ➔ Fournir des informations fiables et objectives, sans chercher à obtenir des informations ou des décisions en exerçant une quelconque pression.
- ➔ Ne pas chercher à obtenir un avantage politique ou réglementaire indu.
- ➔ Veiller à ce que les représentants d'intérêts exercent leurs activités dans le respect du présent Code et de la réglementation applicable.

Dons, mécénat et sponsoring

Le Groupe Eurofeu peut être amené à œuvrer en faveur de la société civile en versant des dons et en exerçant des activités de mécénat ou de sponsoring notamment auprès d'organisations caritatives.

Ces dons, activités de mécénat et de sponsoring peuvent être qualifiés d'actes de corruption quand ils sont réalisés dans le but d'obtenir un avantage indu.

Ainsi, les dons, activités de mécénat et de sponsoring peuvent être utilisés comme un moyen de corrompre une personne susceptible d'influencer une décision dans une transaction, en particulier si cette personne a un intérêt familial avec l'organisation qui reçoit la donation ou le sponsor.

Les règles à respecter :

- ➔ Les dons, activités de mécénat et de sponsoring sont autorisés sous réserve du respect des lois et réglementations applicables.
- ➔ Les dons, activités de mécénat et de sponsoring ne doivent jamais intervenir au profit de personnes physiques.
- ➔ Les dons, activités de mécénat et de sponsoring ne doivent pas être réalisés pour obtenir un avantage indu ou influencer indûment une décision. Ils doivent être conformes aux principes et règles internes du groupe et ne jamais servir à avantager indûment, influencer abusivement ou donner l'apparence d'influencer abusivement quelque décisionnaire que ce soit.
- ➔ Toute opération de ce type doit faire l'objet d'une demande auprès de la Direction afin de n'engager aucun financement qui pourrait nuire à la réputation de l'Entreprise. L'attribution de financement spécifique doit s'effectuer de manière transparente et en coordination avec le service Marketing/Communication.

Financement d'activités politiques

Le financement d'activités politiques désigne toute contribution directe ou indirecte ayant pour but d'apporter un soutien à un parti politique, un candidat ou un élu.

Cette contribution peut consister en un versement d'argent ou tout autre avantage tels que des cadeaux ou des prestations, de la publicité ou toute autre activité partisane.

Le financement d'activités politiques peut être utilisé pour dissimuler un avantage indu afin d'obtenir ou de maintenir une transaction ou relation commerciale. En d'autres termes, le financement d'activités politiques peut être considéré ou interprété comme de la corruption directe ou indirecte.

Les règles à respecter :

- ➔ Toute contribution, financière ou en nature, directe ou indirecte, versée par le Groupe Eurofeu ou par ses Collaborateurs en son nom à des organisations, partis ou personnalités politiques est interdite.
- ➔ Les Collaborateurs doivent séparer leurs activités politiques personnelles de leur mission au sein du Groupe, afin d'éviter toute situation pouvant générer un conflit d'intérêts. Bien évidemment, chaque Collaborateur peut prendre part à des activités politiques de manières personnelles sur son temps libre, en dehors des lieux de travail, avec ses propres ressources financières et sans qu'il soit fait référence, de quelque manière que ce soit, à l'appartenance au Groupe.

Acquisitions, prise de participation et joint-ventures

Lors d'acquisition de sociétés, d'acquisition d'actifs portant sur une branche complète d'activité, de prise de participations, de fusion ou de mise en place de joint-ventures, il convient de s'assurer que la cible ou le partenaire n'a pas ou n'a pas eu de comportement répréhensible au regard des lois anticorruption applicables, et respecte la législation en vigueur en ce domaine.

En effet, dans les opérations précitées, la responsabilité civile ou pénale du Groupe Eurofeu pourrait être engagée et entraîner d'importantes répercussions commerciales, financières et réputationnelles.

Les règles à respecter :

- ➔ Inclure un volet anticorruption au sein des processus d'audit préalables (« due diligences ») dans le cadre d'acquisitions, de prises de participations ou de mise en place de joint-ventures.
- ➔ Inclure une clause anticorruption au sein des contrats et conventions conclus dans le cadre d'acquisitions, de prises de participations ou de mise en place de joint-ventures.

Tenue et exactitude des livres et registres

Les livres et registres désignent ici tous les enregistrements comptables, financiers et commerciaux. Ceux-ci incluent les comptes, correspondances, synthèses, livres et autres documents relatifs à la sphère comptable, financière et commerciale.

Dans le cadre de la lutte contre la corruption, il est essentiel que les transactions soient transparentes, documentées de façon exhaustive et affectées à des comptes qui reflètent leur nature avec précision.

Les règles à respecter :

- Aucune inscription dans les livres et registres du Groupe Eurofeu ne doit être infondée, erronée, falsifiée ou factice.
- Les livres et registres du Groupe doivent être le reflet fidèle et exact des transactions effectuées et devront être établis conformément aux normes et référentiels comptables en vigueur.
- Le principe de séparation des fonctions de décision et de paiement doit être respecté et la traçabilité des paiements assurée.
- Tous les contrôles et procédures d'approbation mis en place au sein du Groupe doivent être appliqués.
- Il convient donc de conserver la documentation démontrant le caractère approprié des prestations concernées et des paiements correspondants.

Données à caractère personnel

Le groupe Eurofeu s'est doté d'une charte de protection des données à caractère personnel de ses clients, salariés et fournisseurs. Elle fournit un cadre de référence à l'ensemble des collaborateurs du Groupe amenés à traiter ce type de données.

Cette Charte rappelle les engagements pris par Eurofeu ainsi que les bonnes pratiques à observer afin de garantir la protection de ces données.

Toute personne a droit au respect de sa vie privée. Les données personnelles ne doivent être recueillies, traitées et conservées que pour un usage déterminé et légitime. Ces informations doivent être portées à la connaissance des personnes concernées.

Les règles à respecter :

- ➔ S'assurer de l'utilité, de la pertinence des informations collectées et de la licéité, loyauté et transparence des traitements de données personnelles des clients, fournisseurs et collaborateurs du groupe ;
- ➔ Garantir le droit au respect de la vie privée des collaborateurs, notamment en ne transmettant pas d'informations à des personnes non habilitées et en s'assurant que les données personnelles sont conservées de façon sécurisée ; En cas de recours à de la sous-traitance, s'assurer que les prestataires respectent ces mêmes principes.
- ➔ Dès le démarrage d'un projet informatique, intégrer la Direction des Services d'Information (DSI) et le Data Protection Officer (DPO), afin de s'assurer du respect de l'ensemble des règles sur la protection des données à caractère personnel ;
- ➔ Assurer la bonne adéquation d'un projet avec les principes de la charte : sécurité, finalités, utilité, etc. ; En cas de doute, toujours contacter le DSI ou le DPO.
- ➔ Toujours traiter les données à caractère personnel pour les finalités prévues dans la Charte, avec confidentialité et en informant la personne concernée au préalable ;

Le respect du code anticorruption et les sanctions applicables

L'interprétation et le respect du Code

Chaque Collaborateur du Groupe Eurofeu, tel que défini dans le préambule, doit lire, comprendre et respecter le présent Code. L'équipe de direction du Groupe veille à sa diffusion et à son respect par les Collaborateurs.

Pour toute question relative au présent Code ou en cas de difficulté d'interprétation s'agissant de son application à une situation donnée, les Collaborateurs sont invités à se rapprocher de leur responsable hiérarchique direct ou indirect.

Le dispositif d'alerte professionnelle

Il est rappelé que le Groupe Eurofeu met en place un dispositif d'alerte professionnelle visant à renforcer les moyens d'expression de l'ensemble des Collaborateurs afin que ces derniers puissent **signaler l'existence de conduites ou de situations contraires au présent Code**.

Si le recours à la voie hiérarchique directe ou indirecte est toujours possible, le dispositif d'alerte professionnelle offre aux Collaborateurs des garanties renforcées de protection en cas d'émission d'un signalement. Son utilisation demeure néanmoins facultative.

En pratique, tout Collaborateur peut adresser son signalement, en utilisant l'adresse dédiée : alerte@eurofeu.fr

Les règles relatives au fonctionnement du dispositif d'alerte professionnelle et les garanties offertes aux Collaborateurs dans le cadre de son utilisation sont détaillées dans les Règlements intérieurs des sociétés concernées.

Les conséquences en cas de violation du Code

Le non-respect des règles édictées au sein du présent Code peut avoir des conséquences graves, non seulement pour le Groupe, mais également pour les Collaborateurs.

Pour le Groupe Eurofeu, tout comportement contraire aux règles posées dans le présent Code pourrait, non seulement porter atteinte à sa réputation et affecter ses activités, mais également l'exposer à devoir réparer le préjudice éventuellement causé, et, l'exposer à des poursuites pénales.

Pour les Collaborateurs, lorsque les circonstances le justifient, le manquement aux règles de lutte contre la corruption figurant dans le Code peut les exposer à des sanctions disciplinaires pouvant aller

jusqu'à la rupture du contrat de travail dans les conditions prévues au règlement intérieur, ainsi qu'à des poursuites, à titre personnel, pénales et/ou civiles.