CODE DE CONDUITE DU GROUPE

Version n°3

SODIAAL

Coopérative Laitière Française

2022

SOMMAIRE

COMMENT L'UTILISER ?

LE CODE DE CONDUITE EST UN OUTIL DE RÉFÉRENCE QUI PERMET À CHACUN D'ENTRE NOUS D'AGIR AVEC INTÉGRITÉ EN S'INTERROGEANT SUR LES SITUATIONS RENCONTRÉES DANS SON ACTIVITÉ

Certaines situations sont difficiles à gérer. Prendre des décisions éthiques semble parfois difficile, car cela implique bien plus que le simple respect d'un ensemble de règles.
Le Code de conduite est un outil de référence qui permet à chacun d'entre nous d'agir avec intégrité en s'interrogeant sur les situations rencontrées dans son activité. En plus du Code de conduite, Sodiaal a mis en place un ensemble de politiques et procédures que nous devons respecter. Enfin, pour prendre la bonne décision, il ne faut pas hésiter à poser des questions chaque fois que nécessaire, afin d'agir comme il convient, au bon moment et pour les bonnes raisons.
Dans certaines situations, il est possible que les orientations données dans le présent Code de conduite, diffèrent de la législation ou des coutumes locales d'un pays. Si la loi ou les coutumes locales imposent des normes plus restrictives que celles définies dans le Code, la loi ou les coutumes locales doivent prévaloir. Si, en revanche, le Code prévoit une disposition plus restrictive, celui-ci prévaudra.

EN CAS DE DOUTE, POSEZ-VOUS LES QUESTIONS SUIVANTES :

- Suis-je en violation d'une loi, du Code de conduite de Sodiaal, de ses politiques et procédures ?
- Suis-je cohérent(e) avec les valeurs éthiques ?
- Est-ce que je me comporte avec les autres comme je souhaiterais que l'on se comporte avec moi ?
- Suis-je redevable de quoi que ce soit envers quelqu'un ?
- Ma décision pourrait-elle sembler inconvenante si elle était publiée en première page d'un journal ?

SI LA RÉPONSE À L'UNE DE CES QUESTIONS SUSCITE DES INQUIÉTUDES, NE LE GARDEZ PAS POUR VOUS, **PARLEZ-EN.**

COMMENT ALERTER ? (voir « Alerte Ethique »).
> Téléphone alerte : 0800 94 16 50
> Adresse mail alerte : conformite@groupesodiaal.fr

Il appartient à chacun d'entre nous d'en connaître et d'en comprendre le contenu. Si nous pensons que l'un ou plusieurs de nos principes éthiques ne sont pas respectés, nous avons le devoir de le signaler.

Le présent Code de Conduite définit les principes directeurs guidant le développement et la construction du Groupe Sodiaal : Il s'applique à chaque collaborateur qui doit en conséquent agir avec discernement dans toutes les situations critiques qu'il peut rencontrer dans ses relations tant à l'intérieur qu'à l'extérieur de l'entreprise.
Le Code de Conduite est intégré au Règlement Intérieur du Groupe.
Il a été validé en séance Comex le 22 août 2022.
En cas de doute sur l'application ou l'interprétation d'une règle, consultez la Direction du Contrôle Interne et de la Conformité avant d'agir.

I.

LES ESSENTIELS DU GROUPE SODIAAL

Sodiaal est une coopérative qui rassemble 20 000 éleveurs laitiers et 10 000 collaborateurs. Notre modèle coopératif repose sur des valeurs humaines fortes, où l'Homme occupe une place centrale dans l'organisation, et également sur des valeurs éthiques qui nous fédèrent :

> la solidarité et l'équité
> le respect
> la confiance
> la transparence
> l'audace

Ces valeurs, partagées par tous, doivent conduire chacune de nos actions au quotidien dans l'accomplissement de notre mission : « *valoriser le lait de tous les sociétaires afin de leur garantir un revenu qui rémunère au mieux leur travail, d'accroître et de partager la profitabilité de l'entreprise de façon durable* ».
Aussi, pour réaffirmer cet engagement dans le respect de ses valeurs auprès de ses collaborateurs, de ses clients, de ses fournisseurs et autres parties prenantes, le Groupe Sodiaal a établi ce Code de Conduite qui précise les bonnes pratiques à suivre individuellement et collectivement pour contribuer pleinement à la réussite de notre modèle coopératif et de notre projet d'entreprise.

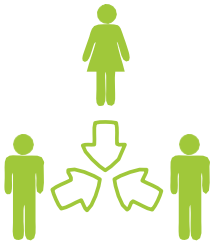
Le Code de Conduite exprime la responsabilité du Groupe Sodiaal envers l'ensemble des parties prenantes de son métier qui sont :

1.Les collaborateurs

Le Groupe Sodiaal entend promouvoir et assurer le maintien d'un environnement de travail stimulant, créatif et non discriminatoire pour l'ensemble des collaborateurs et des partenaires, dans le respect de la diversité et de la dignité de l'individu.
A tous les échelons, le Groupe Sodiaal s'attache à maintenir des relations humaines à la fois exigeantes et respectueuses. Dans ce cadre, il est de la responsabilité de chacun de permettre à tous les collaborateurs d'exercer leur métier dans de bonnes conditions physiques et morales. Dans l'exercice des responsabilités et des relations hiérarchiques, la personne doit toujours être respectée.

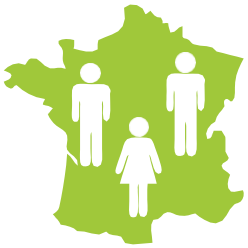
2.Les consommateurs et les clients

Le Groupe Sodiaal veille à la sécurité alimentaire et à la qualité de ses produits, au respect des dispositions légales, réglementaires et des procédures internes. Nos produits doivent être consommés sans risque pour la santé.



3.Les fournisseurs, prestataires et partenaires

Le Groupe Sodiaal conditionne l'exercice de ses relations commerciales au respect des législations locales, des chartes internes et des standards internationaux dans le domaine des droits de l'Homme et des conditions de travail, de l'environnement et de l'éthique.
Le Groupe Sodiaal s'engage à construire une relation équitable et durable avec ses fournisseurs en s'appuyant sur la Charte Relation Fournisseur Responsable, développée par la Médiation des Entreprises et signée par le Groupe.
Le Groupe Sodiaal demande également aux fournisseurs et partenaires de s'engager à respecter le Code de Conduite du Groupe Sodiaal, à agir contre la corruption sous toutes ses formes, contre le travail des personnes mineures, le travail forcé, et à respecter le nouveau règlement général de protection des données personnelles (RGPD).



4.Les fonctionnaires et les représentants de l'Etat

Le Groupe Sodiaal s'attache à établir des échanges fondés sur l'honnêteté et l'intégrité et veille notamment au strict respect des lois et des réglementations.

Ces engagements doivent se traduire par l'implication et le comportement éthique de chaque collaborateur du Groupe en toute circonstance.

5.Une conduite responsable à l'égard des territoires d'intervention

Dans son développement à l'international, le Groupe Sodiaal s'attache à adopter une conduite responsable à l'égard des pays dans lesquels il opère.

Le Groupe Sodiaal veille à ce que ses filiales se conforment aux lois et règlements applicables dans chacun des pays dans lequel il opère.

Le Groupe Sodiaal veille notamment à ce que son développement international s'inscrive dans le respect des environnements naturels et des cultures de ses territoires d'implantation.

Le Groupe Sodiaal participe par ses activités au développement économique et social des communautés où se trouvent ses implantations, dans un souci de développement à long terme.

Le Groupe Sodiaal s'interdit de prendre tout engagement ou support de quelque nature que ce soit en faveur d'un parti, d'un groupe politique ou religieux.

II

TRAVAIL EN ENTREPRISE

Le Groupe Sodiaal favorise des relations entre collègues fondées sur la courtoisie, la considération, la reconnaissance et la discrétion. Il condamne le harcèlement, de quelque manière que ce soit.
Respectueux de la diversité et de la vie privée, le Groupe Sodiaal considère avant tout la compétence de ses collaborateurs et s'interdit toute forme de discrimination.
Le Groupe Sodiaal s'attache également à la diversité au sein de son organisation et considère les différences entre ses collaborateurs comme une richesse indispensable à la réussite d'une entreprise responsable.
De plus, le Groupe Sodiaal favorise la diversité et l'égalité des chances pour chaque collaborateur ou candidat en matière de recrutement, d'accès à la formation, de rémunération, de protection sociale, de mobilité interne et d'évolutions professionnelles.

1.Responsabilité personnelle

Chaque collaborateur doit s'acquitter de ses tâches avec honnêteté, soin, diligence, professionnalisme, impartialité et éthique.

2.Respect des lois et réglementations

Chaque collaborateur du Groupe Sodiaal doit connaître les lois, les réglementations et obligations liées à sa tâche. Toute activité risquant d'entraîner le Groupe dans une pratique illicite est rigoureusement proscrite.

3.Relations avec les clients

Le Groupe Sodiaal s'attache à traiter honnêtement et équitablement tous ses clients, quelle que soit la taille de l'entreprise.

Il s'engage à fournir à ses clients des produits et services de qualité répondant à leurs exigences. Les informations confidentielles, sensibles ou privées relatives aux clients ne doivent en aucun cas être communiquées à autrui par un collaborateur du Groupe Sodiaal, sauf lorsque cela est exigé par une autorité compétente, ou autorisé dans le cadre d'un projet ou d'un contrat.

4.Relations avec les fournisseurs

Les relations humaines sont considérées comme un atout majeur pour le Groupe Sodiaal qui souhaite que ses échanges avec ses fournisseurs riment avec engagement et partage de valeurs communes.
Les attentes du Groupe Sodiaal vis-à-vis de ses fournisseurs se portent prioritairement sur la qualité de leurs prestations et de leurs produits.
Le fournisseur s'engage à respecter et à faire respecter les engagements du Groupe Sodiaal par l'ensemble de ses collaborateurs, ainsi que par toute personne ou entité impliquées dans l'exécution des contrats conclus entre lui et notre Groupe.

III
SANTE ET SECURITE

La Santé et la Sécurité font partie des priorités du Groupe dans le cadre de la mise en œuvre de sa politique « Sécurité d'Abord ».
Ainsi, le Groupe Sodiaal s'engage à garantir un environnement de travail sûr et sain dans l'ensemble de ses sites, avec un niveau d'exigence équivalent pour chacun des sites. Le Groupe Sodiaal réalise les efforts nécessaires pour assurer la protection des collaborateurs, développer les bonnes pratiques et corriger les conditions à risque quel que soit leur lieu de travail.

Afin de s'assurer de la mise en pratique de comportements adaptés en matière de sécurité, le Groupe Sodiaal met en œuvre des « Visites Comportementales de Sécurité ». Il s'agit d'un outil de management et d'un moment d'échange entre collaborateurs et managers permettant d'étudier les méthodes, les organisations et l'environnement de travail en situation réelle. Les collaborateurs formés s'engagent à effectuer ces visites.

Chaque collaborateur a l'obligation de signaler les situations dangereuses dont il est témoin ou les incidents qui en sont révélateurs, et de contribuer à la mise en œuvre des actions préventives. Le respect des consignes de sécurité est une obligation stricte.

Cet engagement est aussi valable pour les entreprises intérimaires, les entreprises extérieures et les visiteurs.

IV

ENVIRONNEMENT ET RESPONSABILITE SOCIETALE

1.Environnement

Le respect de l'environnement est une priorité pour le Groupe Sodiaal.

Le Groupe Sodiaal s'engage à respecter les règlements et normes en vigueur en matière d'environnement, notamment en termes de :

- consommation d'énergies, d'eau et de produits chimiques,
- émission dans l'air, rejets liquides, nuisances sonores et olfactives et pollutions du sol
- traitement des déchets
- préservation de la biodiversité…

Il cherche à constamment améliorer la gestion de ses activités d'un point de vue environnemental, et travaille notamment à la réduction de son empreinte carbone tout au long de la chaine et à la conception et la mise sur le marché d'emballages recyclables.

2.Responsabilité sociétale

Le Groupe Sodiaal est engagé dans une démarche d'amélioration continue, qui vise à toujours mieux connaitre et réduire les impacts environnementaux et sociétaux liés à ses activités. Cette démarche est structurée autour de 3 thématiques, dans le but de couvrir l'ensemble des enjeux prioritaires identifiés pour le Groupe (voir ci-après).

En ce qui concerne le périmètre amont de la filière et la production du lait sur les fermes de nos éleveurs-adhérents, le Groupe Sodiaal a mis en place depuis 1998 une démarche volontaire appelée « La Route Du Lait ». L'ensemble des éleveurs-adhérents de Sodiaal sont concernés et sont ainsi engagés en faveur de la qualité des produits, dans le respect du développement durable, et la prise en compte des garanties sanitaires, d'hygiène, de bien-être des animaux, de respect de l'environnement et des bonnes pratiques d'élevage.

ELEVAGES

TOURNÉS VERS L'AVENIR

Bons pour les hommes
Création & partage de la valeur, collecte pérenne, jeunes agriculteurs

Préservant la planète
Elevages bas carbone, haute biodiversité, résilients & autonomes

Respectueux des animaux
Exemplarité en matière de bien-être animal, alternatives aux antibiotiques

PRODUITS

POUR LE MEILLEUR DU LAIT

Apportant le meilleur à nos consos
Qualité, nutrition, naturalité

Faible empreinte environnementale
Empreinte carbone, eau, emballages, lutte contre le gaspillage alimentaire

Achats responsables
Evaluation fournisseur, filières responsables, charte & éthique

COMMUNAUTE

FIERE ET ENGAGEE

Qualité de vie au travail
Santé et sécurité, non-discrimination, bien-être au travail

Esprit de communauté
Fierté d'appartenance, ouverture du capital

Parcours & expertises
Mobilité professionnelle, formations, transmission interne

Chaque collaborateur est encouragé à prendre connaissance des engagements du Groupe Sodiaal en matière de responsabilité sociétale et environnementale et à faire son possible pour contribuer à les respecter dans le cadre de son activité.
En complément, nos fournisseurs s'engagent à respecter et faire respecter ces engagements sur leur propre périmètre de responsabilité, conformément aux dispositions en vigueur sur les territoires où ils exercent leurs activités.

La Déclaration de Performance Extra-Financière (DPEF), auditée par un organisme tiers indépendant et publiée annuellement, rend compte des engagements du Groupe Sodiaal, de leur éventuelle mise à jour, ainsi que des principales actions et réalisations de l'année écoulée en matière de responsabilité sociétale et environnementale.

3.Non gaspillage

Tous les collaborateurs sont encouragés et sensibilisés à faire un usage approprié des ressources mises à leur disposition, tout en respectant les nécessités liées à leur activité.

Dans le cadre de la loi dite « devoir de vigilance » (2017), le Groupe Sodiaal publie annuellement son plan de vigilance afin d'identifier et de prévenir les risques d'atteintes graves à l'environnement, aux libertés fondamentales, et à la santé et la sécurité des personnes pouvant résulter des activités du Groupe, de ses filiales et de ses fournisseurs et prestataires.
Il est possible de trouver, dans le plan de vigilance, des informations inhérentes à l'Ethique des affaires, la Responsabilité Sociétale de l'Entreprise, la santé-sécurité au travail ainsi que notre mécanisme d'alerte.

V

INTEGRITE DANS LES AFFAIRES

1.Lutte contre corruption

Le Groupe Sodiaal et ses fournisseurs s'engagent à respecter les obligations prévues par la loi n° 2016 1691 dite loi Sapin 2, publiée au Journal Officiel le 10 décembre 2016 et a mis en place différents moyens pour prévenir et lutter contre toute pratique de corruption.
La corruption suppose :
l'octroi d'un avantage quelconque (argent, promesse, dons, cadeaux, suppression de dettes, sous-facturation, invitations…)

- à une personne privée ou publique pouvant influer sur une décision
- pour qu'elle accomplisse ou n'accomplisse pas un acte lié à son activité ou sa fonction

La corruption est interdite qu'elle soit active (corrupteur) ou passive (corrompu).
Toutes les pratiques de corruption y compris les tentatives, sont interdites et lourdement sanctionnées par la loi (emprisonnement, amende, déchéance des droits civils et civiques notamment).
Les conséquences de telles pratiques sur le Groupe Sodiaal, notamment en termes de réputation commerciale et d'image, seraient extrêmement préjudiciables.

2. Dons, sponsoring et contributions politiques

Les dons et le sponsoring sont des cadeaux versés dans un but caritatif ou pour soutenir une cause précise. Il peut s'agir d'argent, de services, d'articles neufs ou usagés, ou encore d'aide humanitaire ou d'urgence, de soutien au développement et d'assistance médicale. Dans le cas du sponsoring, le soutien de l'entreprise se fait le plus sou- vent en échange de différentes formes de visibilité.

En tant que Groupe citoyen et responsable, le Groupe Sodiaal entend soutenir le développement des populations et des communautés mais s'engage à ce que ses activités de dons et de sponsoring soient réalisées dans le strict respect des lois anticorruption applicables.

Afin de garantir l'impartialité de la vie politique, le Groupe Sodiaal ne verse aucun fonds et ne fournit aucun service aux partis politiques, aux titulaires d'un mandat public ou candidats à un tel mandat, quand bien même le caractère licite de telles contributions serait reconnu en vertu des lois du pays où de tels versements seraient susceptibles d'être faits.

QUELQUES EXEMPLES DE SITUATIONS À RISQUE :

✗ Demande de financement d'un club ou d'une association sportive ou en échange d'une promesse de traitement préférentiel dans le cadre d'un marché public ou privé.
✗ Promesse d'emploi ou de contrat de stage contre l'achat de produit ou l'acceptation d'un prix supérieur.
✗ Cadeaux, invitations dans l'espoir de la signature d'un contrat ou l'obtention d'une autorisation.

3.Trafic d'influence

Infraction très proche de la corruption, mais qui suppose d'utiliser un intermédiaire agent public.
Trafic d'influence : une personne tierce, agent public, intervient auprès d'une autorité ou d'une administration publique pour obtenir une décision. L'intermédiaire se présente comme une personne dotée d'influence pour obtenir une faveur réelle ou supposée.
De façon plus précise, il est rappelé que le Groupe Sodiaal a déjà mis en place les règles suivantes qui doivent être respectées par l'ensemble des collaborateurs du Groupe :

RELATION AVEC UN DÉTENTEUR DE MANDATS OU POUVOIRS PUBLICS ET/OU SES REPRÉSENTANTS

Tout collaborateur du Groupe qui entre en communication avec des personnes occupant des fonctions administratives ou gouvernementales dans le cadre d'activités de représentation d'intérêt doit respecter les réglementations s'appliquant dans les pays dans lesquels il opère. Toute pratique de représentation d'intérêts pour le compte du Groupe doit notamment être dûment documentée avec transmission de la documentation à la Direction du Contrôle Interne et de la Conformité pour conservation.

Règles à appliquer :

- Toute relation de nature à obtenir un avantage particulier est interdite.
- Toute relation professionnelle dépassant le seuil des 10 rencontres par an avec un même représentant d'intérêt doit être prohibée.
- Les relations ayant trait à la sécurité des biens et des personnes sont autorisées et ne rentrent pas dans le cadre de ce suivi.

LUTTE CONTRE LES PAIEMENTS ILLICITES

La politique du Groupe Sodiaal est de bannir les paiements et pratiques illicites sous toutes leurs formes (en France comme à l'Etranger). Les entreprises et les collaborateurs du Groupe ne doivent pas offrir un avantage ni répondre à la sollicitation de toute personne qui, prétendant disposer d'une influence réelle ou supposée auprès d'une personne publique ou privée, proposerait d'user de son influence directe ou indirecte, en vue d'obtenir des marchés ou une décision quelconque.

4.Cadeaux et Invitations

Les cadeaux, invitations et repas ne peuvent être ni acceptés ni offerts dès lors qu'ils dépassent le montant fixé qui est de 60 euros par personne et par an.
Lorsque pour des raisons impérieuses il est difficile de respecter la limite fixée, il est alors impératif d'être totalement transparent, de déclarer à son responsable hiérarchique et d'inscrire sur un registre ad hoc tout cadeau, reçu ou toute invitation reçue (valeur appréciée de bonne foi) ou donné(e), dépassant le montant limite fixé par le Groupe.
Le registre doit être renseigné de telle façon à pouvoir être lisible par un tiers à l'entreprise et spécifiquement un organe de contrôle.

Règles à appliquer uniquement pour les cadeaux et invitations externes au Groupe Sodiaal : un cadeau offert ou reçu ne peut pas dépasser le seuil maximal fixé sauf accord préalable du responsable hiérarchique dument matérialisé (manuscrit ou mail à conserver par chaque responsable de service). Cela concerne tous types de cadeaux, par exemple :

- Invitation à un repas ; en cas de doute sur la valeur d'une invitation reçue, il est préférable par précaution de demander l'accord préalable du responsable hiérarchique

- Invitation à une manifestation sportive ou culturelle
- Invitation à un événement commercial, de relation publique ...
- Chèques cadeaux
- Cadeau de fin d'année
- Toute invitation avec le conjoint
- Toute invitation dont la valeur excède 60 €
- Toute répétition au-delà de 4 invitations de la part de la même personne
- … etc.

Un cadeau reçu ou une invitation reçue supérieur à la limite fixée (60 euros par an et par personne) doit être si possible refusé spontanément. S'il est accepté, il doit être porté au registre même en cas de distribution ou de partage avec d'autres collaborateurs. La mention « a été distribué ou partagé » doit être inscrite sur le registre, ainsi que le service ou les destinataires concernés.

Tous les cadeaux offerts ou reçus doivent être mentionnés au registre dès lors qu'ils dépassent la limite fixée.

Les pratiques suivantes ne sont pas autorisées :

- Offrir un cadeau ou un divertissement à un agent officiel afin de faciliter certaines démarches.
- Offrir un cadeau ou un divertissement pour influencer une décision commerciale/gouvernementale.
- Inviter un des membres de la famille d'un client/fournisseur déjà en relation d'affaire ou potentiel à assister à un événement culturel, sportif…
- Accepter une invitation avant ou pendant un appel d'offre sur lequel on peut avoir une action/influence.
- Payer personnellement un cadeau ou un divertissement afin d'éviter d'avoir à respecter le Code de Conduite.
- Obtenir des réductions sur des produits ou services qui ne sont pas proposés à tous les collaborateurs.
- Obtenir des cadeaux ou divertissements de nature inappropriée ou dans des lieux inadéquats.

TYPES DE PRATIQUES ET COMPORTEMENTS INTERDITS

✗ Demande de financement d'un club ou d'une association sportive ou en échange d'une promesse de traitement préférentiel dans le cadre d'un marché public ou privé.

✗ Promesse d'emploi ou de contrat de stage contre l'achat de produit ou l'acceptation d'un prix supérieur.

✗ Cadeaux, invitations dans l'espoir de la signature d'un contrat ou l'obtention d'une autorisation.

BONNES PRATIQUES ET COMPORTEMENTS AUTORISÉS

✔ Respect de l'image de marque et de la bonne réputation du Groupe Sodiaal

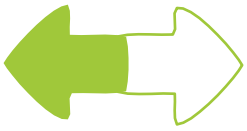
✔ Respect des règles d'éthique mis en place par le Groupe Sodiaal, de loyauté et de transparence

✔ Refus clair et net de toute proposition de corruption active et passive ou de fraude ou de conflit d'intérêts

✔ Utilisation si nécessaire du système d'alerte mis à la disposition des collaborateurs du Groupe Sodiaal. (Cf. page 34)

✔ Respect des lois et règlements applicables dans les pays d'activité

✔ Respects des cultures et des environnements dans les pays d'activité



5.Conflits d'intérêts

Un conflit d'intérêts est une situation dans laquelle les intérêts du Groupe Sodiaal divergent des intérêts personnels de nos collaborateurs ou de leurs proches. Nos collaborateurs ne doivent pas se trouver dans des situations ne leur permettant pas de rester objectifs et impartiaux dans l'exercice de leurs fonctions.

Ils doivent alerter leur hiérarchie en cas de situation potentielle de conflit d'intérêts et ne doivent pas interférer dans la prise de décision.

6.Droit de la concurrence

Le Groupe Sodiaal respecte les dispositions légales et réglementaires, nationales et internationales, relatives au droit de la concurrence afin d'avoir des échanges justes et loyaux s'inscrivant dans le cadre d'une concurrence libre.

Le droit de la concurrence a pour objectif de protéger le fonctionnement d'une concurrence saine et loyale entre les entreprises.

Le droit de la concurrence sanctionne lourdement les comportements d'entreprises ou de collaborateurs d'entreprises qui faussent le jeu d'une concurrence loyale, au détriment des clients et des fournisseurs et au final des consommateurs.

En cas d'infraction aux règles de concurrence, l'Autorité de la concurrence au niveau français et la Commission au niveau européen peuvent prononcer des amendes très élevées et des injonctions de cessation et de modification du comportement. Les juridictions de droit commun peuvent condamner l'entreprise en infraction aux versements de dommages et intérêts et infliger des sanctions pénales aux personnes physiques si celles-ci ont pris intentionnellement une part personnelle et déterminante dans la conception, l'organisation et la mise en œuvre des pratiques anticoncurrentielles (jusqu'à 75 000 euros d'amende et 4 ans d'emprisonnement).

Le Groupe Sodiaal a pris deux engagements fondamentaux : adopter un comportement libre et concurrentiel et mettre en œuvre un programme de conformité au droit de la concurrence dont les principaux éléments sont les suivants :

- **Engagement des dirigeants et sensibilisation du personnel**
- **Nomination d'une Directrice du programme de la conformité**
- **Mise en place de modules de formation aux règles du droit de la concurrence, dont une formation annuelle par e-learning**
- **Adaptation du règlement intérieur pour mentionner les sanctions encourues en cas d'une participation à une violation des règles de concurrence**
- **Création d'un dispositif de prévention d'alerte**
- **Insertion dans les contrats de travail des dispositions spécifiques concernant le respect des règles de concurrence, le suivi des informations et la participation au dispositif d'alerte**
- **Associer nos fournisseurs à nos démarches éthiques**

Le droit de la concurrence interdit les ententes et les abus de position dominante.

LES ENTENTES ANTICONCURRENTIELLES

Les ententes illicites sont constituées de tous accords, formels ou informels, entre entreprises indépendantes ayant pour objet ou pour effet de restreindre la concurrence sur un marché.

Il existe deux sortes d'ententes :

- Les ententes horizontales : il s'agit d'accords écrits, verbaux, tacites, informels, passés entre des concurrents.
- Les ententes verticales : il s'agit d'accords écrits, verbaux, tacites, informels, passés entre entreprises indépendantes situées à des niveaux différents de la chaîne commerciale (par exemple : entre un fournisseur et son distributeur)

LES ABUS DE POSITION DOMINANTE

Les abus de position dominante émanent d'une entreprise qui use de sa position de force sur un marché pour le verrouiller, pour évincer ses concurrents ou pour empêcher l'arrivée de nouveaux entrants.

Deux conditions sont nécessaires : l'existence d'une position dominante et celle d'un abus.

Il existe plusieurs critères pour démontrer l'existence d'une position dominante, les principaux sont les suivants :

- La part de marché de l'entreprise à l'origine des pratiques
- L'écart existant entre la part de marché de l'entreprise en cause et celle de ses concurrents
- L'image de marque, la notoriété de l'entreprise...

Parmi les abus figurent notamment : le refus de vente ou de prestations de services sans raison objective, la pratique de prix prédateurs, excessifs ou imposés, les ventes liées, les remises de fidélité, les exclusivités, les pratiques discriminatoires et dénigrement…

LES PRATIQUES ET COMPORTEMENTS INTERDITS

Dans les relations avec les entreprises concurrentes :

✗ Les échanges d'informations sensibles (prix d'achat, prix de vente, volume, marges, stratégies, coûts, suivi de négociations avec la distribution)

✗ Les accords même tacites qui impliquent la fixation en commun de prix ou de conditions commerciales, la répartition de marchés géographique ou de clientèle, la limitation de la production, des capacités, des débouchés, des investissements ou des progrès techniques

✗ La discussion ou concertation entre concurrents avant le dépôt des offres

✗ La participation au boycott d'un client ou d'un fournisseur

✗ L'accord ou la discussion sur un prix moyen d'achat des matières premières

Dans les relations verticales avec des clients revendeurs ou des fournisseurs :

✗ Le fait d'imposer un prix de vente minimum ou de fixer la marge du distributeur

✗ Le fait de faire pression/offrir des incitations financières pour que les prix soient alignés sur les prix de vente recommandées.

LES PRATIQUES ET COMPORTEMENTS AUTORISÉS

Dans les relations avec les entreprises concurrentes :

✔ L'utilisation de tendance de prix ou de marché et d'indices en vue de la fixation individuelle des prix

✔ La collecte et /ou la transmission au sein des organisations professionnelles d'informations sur les prix et les volumes passés (6 mois ou +) et agrégés ou l'information publiquement disponible (presse …)

✔ La mise en place des plans de maîtrise des volumes de fromages pour notamment mieux gérer les volumes de lait en fonction des volumes AOP que la filière AOP peut vendre

✔ La réalisation d'études de marchés

Dans les relations verticales avec les clients revendeurs ou les fournisseurs :

✔ La transmission de prix de vente recommandés à condition qu'elle ne soit pas répétée

✔ L'explication de la politique de prix

✔ La négociation de remises et ristournes

RECOMMANDATIONS PRATIQUES :

Lors de réunions officielles ou d'échanges informels avec les différents acteurs du marché :
S'assurer que les réunions soient organisées selon un ordre du jour qui ne fait pas mention de pratiques interdites. S'en tenir à l'ordre du jour. Chaque réunion doit faire l'objet d'un compte rendu. Si des pratiques anticoncurrentielles sont mises en œuvre ou même évoquées pendant la réunion, demander immédiatement l'interruption des discussions, formuler expressément son désaccord et s'assurer qu'il figure dans le procès-verbal de la réunion. Quitter la réunion si besoin et faire constater son départ sur le PV de la réunion.

Lors de la conclusion de certains accords de coopération :
Pour les accords de mise en commun de moyens de production, les accords de coopération industrielle, les accords d'achat groupé, les accords de R&D ou accords de commercialisation en commun et tout accord nécessitant des échanges d'informations entre concurrents, il convient de consulter le service juridique.

En cas d'enquête des autorités de concurrence :
Les enquêtes de concurrence s'apparentent à des perquisitions au cours desquelles les enquêteurs visitent les bureaux, saisissent des documents et peuvent questionner les personnes présentes. Les enquêtes de concurrence sont souvent anxiogènes et il convient alors de garder son calme.

7.Fraude

La fraude consiste à tromper délibérément autrui pour obtenir un bénéfice illégitime, ou pour contourner des obligations légales ou des règles de l'organisation. Un comportement frauduleux suppose donc un élément factuel et intentionnel ainsi qu'un procédé de dissimulation de l'agissement non-autorisé.
Le Groupe Sodiaal ne tolère en aucune manière les pratiques frauduleuses dans le cadre de la conduite de ses activités. Il met en œuvre les mesures nécessaires pour en réduire les risques et les effets.

La lutte contre la fraude est un impératif. Au-delà des risques financiers encourus, le risque de fraude est susceptible de porter atteinte à l'intégrité du Groupe, à sa réputation et à la confiance qui lui est portée par ses clients, affiliés ou toute autre partie.

Vous pouvez donc consulter les engagements du Groupe Sodiaal en matière de lutte contre la fraude dans la Charte de lutte contre la fraude.

EXEMPLES DE SITUATIONS INTERDITES

✗ Lors de la signature d'un contrat avec une entreprise cliente, ses représentants manifestent le souhait de transformer en avantage en nature (par exemple la livraison gratuite de produits) une remise que vous avez accordée.

✗ Pour accroître les chances de réalisation d'une transaction avec des autorités, quelqu'un vous suggère vivement une association avec un partenaire local désigné.

8.Blanchiment d'argent

Le blanchiment d'argent est un processus qui consiste à **dissimuler la nature et la provenance d'argent issu d'activités illicites** (trafic de stupéfiants, trafic d'armes, traite des personnes, fraude fiscale, travail clandestin, corruption, spéculations illégales...) en incorporant cet « argent sale » dans des activités légales. L'objectif est de lui **donner une apparence légale et de dissimuler sa provenance et son propriétaire réel** (via de fausses factures, des sociétés écrans...).

Le **financement du terrorisme** consiste à fournir des biens, des prestations, des services ou des fonds susceptibles d'être utilisés dans le cadre d'activités terroristes.

Le **Groupe interdit et condamne fermement** toutes les pratiques de cette nature.

Le blanchiment de capitaux représente un risque pour Sodiaal, qui ne doit en aucune façon pouvoir être accusé de favoriser le financement d'activités interdites, telles que le terrorisme, le trafic de stupéfiants ou encore le financement de certains partis politiques.
Ce risque est de nature pénale, avec des **peines allant jusqu'à dix ans d'emprisonnement et 750000 euros d'amende** pour les personnes physiques. La révélation d'un tel délit porterait également une **atteinte importante aux intérêts et à l'image de Sodiaal**.

LES PRATIQUES ET COMPORTEMENTS AUTORISES

- ✓ Être en permanence vigilant
- ✓ Réaliser un contrôle d'intégrité de nos relations d'affaires, préalablement à tout engagement, afin de nous assurer qu'il s'agit d'activités légitimes et que l'argent ne provient pas d'activités illégales ou de sources soumises à des sanctions internationales. Obtenir et analyser les pièces justificatives de nos relations d'affaires.
- ✓ Établir un système de veille et d'alerte, concernant notamment les opérations atypiques ou suspectes, les transferts de fonds en provenance ou à destination de zones géographiques considérées comme risquées.
- ✓ Consulter les listes des pays à risque du MAF.
- ✓ Signaler tout soupçon ou doute à votre supérieur hiérarchique ou à la Direction du Contrôle Interne et de la Conformité.

LES PRATIQUES ET COMPORTEMENTS INTERDITS

- × Dissimuler des paiements en ayant recours à des tiers.
- × Accepter des transactions en espèce, sauf cas particulier et en toute transparence avec notre hiérarchie.
- × Accepter les règlements inhabituels sans analyse et vérification préalables des pièces justificatives.

QUELQUES EXEMPLES DE SITUATIONS A RISQUE

- ➢ Les transferts de fonds en provenance ou à destination de zones géographiques considérées comme risquées.
- ➢ Les opérations ou activités nécessitant des règlements en espèces.
- ➢ L'utilisation de « caisses missions ».
- ➢ Les transactions structurées pour contourner les obligations de déclaration ou de reporting.
- ➢ Les opérations inhabituellement complexes ou impliquant des montants inhabituellement élevés.
- ➢ Les virements en provenance ou vers des comptes numérotés.

9.Confidentialité et utilisation de renseignements officiels

La confidentialité des informations est une priorité pour l'entreprise.
Chaque collaborateur veille à protéger les informations sensibles et/ou de nature confidentielle appartenant et/ ou relatives au Groupe Sodiaal et aux entreprises qui le composent, leurs activités, leurs stratégies, leurs poli- tiques, leurs produits ou autres et ce, quel qu'en soit le support ou la nature. Ainsi, tout utilisateur des systèmes d'information et de communication du Groupe Sodiaal doit faire preuve d'un comportement professionnel et responsable, veillant à préserver l'image du Groupe Sodiaal, de ses activités, de ses produits, de ses marques et de ses collaborateurs.

BONNES PRATIQUES ET COMPORTEMENTS AUTORISES

- ✓ Traiter les sujets confidentiels avec la plus grande prudence dans des environnements extérieurs (ex. : en train, en avion, au restaurant, lors de conférences).
- ✓ Demander conseil à la Direction Juridique sur la nécessité d'établir un accord de confidentialité.
- ✓ Signaler à votre hiérarchie toute situation pouvant indiquer que la protection ou la confidentialité des informations sensibles a pu être affectée.

10.Prévention des conflits d'intérêts

Chaque collaborateur se doit d'exercer ses responsabilités avec bonne foi et loyauté à l'égard du Groupe et se doit de veiller à se prémunir contre toute situation de conflit d'intérêts.
Il existe un conflit d'intérêts lorsque, dans le cadre de son activité professionnelle, les intérêts personnels du collaborateur sont directement ou indirectement en contradiction ou en concours avec les intérêts du Groupe et peuvent, dès lors, influencer la position ou la décision qu'il est amené à prendre ou à ne pas prendre et mettre en cause sa loyauté.

Ces intérêts personnels peuvent résulter d'engagements financiers ou professionnels, de lien familiaux ou sentimentaux ou encore de liens d'appartenance politique ou idéologique.

Le conflit d'intérêts n'est pas en droit français un délit. En revanche, c'est l'utilisation frauduleuse qui pourrait découler d'une telle situation qui peut être sanctionnable (prise illégale d'intérêts, favoritisme, corruption, etc.).

QUELQUES EXEMPLES DE SITUATIONS A RISQUE

- ➢ Détenir un mandat électif.
- ➢ Travailler sous quelque forme que ce soit/être en relation d'affaires personnelle avec un client, un fournisseur ou un concurrent du Groupe ou détenir des intérêts significatifs dans ces derniers.
- ➢ Recevoir, directement ou indirectement, des avances, prêts, garanties ou services, cadeaux, dans le but d'influencer une décision du Groupe.
- ➢ Faire affaire au nom du Groupe avec un membre de sa famille ou une entreprise avec laquelle le collaborateur et/ou un membre de sa famille est associé.

LES PRATIQUES ET COMPORTEMENTS AUTORISES

- ✓ Informer sa hiérarchie si des activités sont susceptibles de créer un conflit d'intérêts.
- ✓ Veiller à ce que ses actes et décisions ne soient pas influencés par des intérêts qui pourraient raisonnablement apparaître comme étant en conflit avec ceux du Groupe.
- ✓ En cas de situation potentielle de conflit d'intérêts, se demander si ses intérêts personnels pourraient interférer avec ceux du Groupe et si cela pourrait être perçu comme tel par toute personne interne ou externe à celui-ci.
- ✓ Prévenir sa hiérarchie et la DRH si l'on exerce un mandat électif, un mandat social, une fonction de conseil, ou si l'on occupe un poste à responsabilité chez un concurrent ou partenaire.
- ✓ En cas de doute sur l'existence d'une situation de conflit d'intérêts, référez-en à la Direction du Contrôle Interne et de la Conformité.

TYPES DE PRATIQUES ET COMPORTEMENTS INTERDITS

- × Influencer l'embauche, l'évaluation du travail ou la rémunération d'un proche.
- × Faire un usage abusif de l'influence et des ressources du Groupe.
- × Retenir ou contribuer à faire retenir, pour un marché, une entité dans laquelle nous-mêmes ou l'un de nos proches possédons un intérêt.
- × Utiliser ou partager des informations confidentielles concernant le Groupe, dans notre intérêt personnel ou celui d'un proche.
- × Recourir pour ses contrats personnels à des sociétés partenaires du Groupe selon des modalités autres que celles applicables au grand public.
- × Dissimuler des informations sur tout conflit d'intérêts, même potentiel.

Vous pouvez également consulter les engagements du Groupe Sodiaal en matière d'éthique dans le plan de vigilance, annuellement publié dans le cadre de la loi dite « devoir de vigilance » (2017).

VI

TRAITEMENT DES DONNEES A CARACTERE PERSONNEL

1.Traitement des données à caractère personnel

Une donnée à caractère personnel (DCP) est une notion très large qui englobe toute information se rapportant à une personne physique identifiée ou identifiable.

Il existe 2 types d'identifications :

- identification directe (nom, prénom etc.) ;
- identification indirecte (identifiant, numéro etc.)

Le Groupe Sodiaal s'engage à respecter les règles applicables dans le domaine de la protection des données à caractère personnel, aussi bien à l'égard de ses producteurs, collaborateurs que des tiers, notamment clients, fournisseurs et consommateurs à se conformer aux exigences légales dans ce domaine.

Le Groupe Sodiaal a nommé une déléguée à la protection des données (DPO) et a mis en place le dispositif de protection des données à caractère personnel conforme aux exigences du RGPD (Règlement Général de Protection des Données) incluant notamment :

- Un suivi des traitements des données, afin d'identifier et de répertorier les traitements existants et à en tenir un inventaire exhaustif.
- Une information sur les droits des personnes concernées par les traitements de DCP (in- formation sur la nature et la finalité des traitements les concernant, sur les procédures d'exercices de leurs droits et sur les modalités de recueil de consentements).
- La mise à jour des contrats concernés.
- Un programme de formation e-learning.

Chaque collaborateur du Groupe Sodiaal a l'obligation de se conformer aux règles et dispositifs mis en place :

- Ne plus enregistrer sur le disque dur ou clé USB les fichiers contenant des données à caractère personnel.
- Ne pas faire sortir à l'extérieur de l'entreprise des données à caractère personnel.

2.Règles de bonnes pratiques RGPD

LORS DE LA COLLECTE DE DCP

À FAIRE

- ✓ Identifier précisément les finalités initiales de la collecte des DCP pour les rendre déterminées et explicites.
- ✓ Examiner les formalités réalisées pour le traitement et les mentions d'information pour déterminer si les finalités de la collecte et du traitement des DCP sont déterminées et explicites.
- ✓ Analyser la légitimité des finalités de la collecte et du traitement des DCP.

À NE PAS FAIRE

- ✗ Collecter des DCP dont le responsable de traitement ne connait pas l'origine.
- ✗ Traiter des DCP interdites (santé, religion, opinions politiques, notamment).
- ✗ Collecter des DCP sans informer les personnes sur les finalités de la collecte et du traitement des DCP.
- ✗ Utiliser un traitement pour d'autres finalités sans se poser la question de la compatibilité de ces nouvelles finalités avec les finalités initiales.

QUALITÉ DES DCP

À FAIRE

✓ Mettre à jour périodiquement les traitements et fichiers de données à caractère personnel.

✓ Pour les zones de commentaires libres, s'assurer que seules des DCP nécessaires au traitement sont collectées.

À NE PAS FAIRE

✗ Dans les zones de commentaires libres :
- Appréciations d'ordre personnel, jugements de valeur : expressions injurieuses, désobligeantes, blessantes ;
- Appréciations sur le caractère de la personne (exemples : « personne timide », « mauvais caractère », etc.) ;

✗ DCP sur l'origine raciale, ethnique, opinions politiques, religieuses, philosophiques, appartenance syndicale, santé, vie sexuelle.

DURÉE DE CONSERVATION DES DCP

À FAIRE

✓ Vérifier qu'il existe des durées de conservation pour chaque catégorie de DCP traitées au sein du traitement.

✓ Apprécier la durée de conservation par rapport à la finalité poursuivie.

À NE PAS FAIRE

✗ Procéder à des extractions des données d'une application et conserver ce fichier sans s'assurer de respecter la durée de conservation initiale.

✗ Encourager ou faciliter les extractions Excel.

✗ Ne pas définir de durée de conservation dans les applications lors de la phase de développement.

DESTINATAIRES DES TRAITEMENTS

À FAIRE

✓ Identifier les destinataires de chaque traitement en se référant à la formalité préalable effectuée.

À NE PAS FAIRE

✗ Communiquer les DCP à des tiers sans vérifier leur habilitation.

TRANSFERTS DE DCP

À FAIRE

✓ Identifier les transferts réalisés hors de l'Union Européenne.

✓ Vérifier à quel cadre juridique est soumis le transfert vers les pays identifiés.

À NE PAS FAIRE

✗ Mettre en œuvre des transferts de données vers des pays hors Union Européenne n'ayant pas de protection adéquate sans encadrement juridique.

INFORMATION DES PERSONNES CONCERNÉES

À FAIRE

✓ S'assurer que les personnes concernées ont bien été informées du traitement qui va être mis en œuvre. Le cas échéant, informer les personnes concernées au moyen d'une mention.

À NE PAS FAIRE

✗ Ne pas apposer de mention ou la faire figurer de telle manière qu'elle soit peu visible.

VII
DROIT À LA DÉCONNEXION

Le développement du digital a induit des changements dans l'environnement et les conditions de travail. Si les technologies de l'information et de la communication fluidifient les échanges, améliorent la productivité et permettent d'abolir les barrières spatiales, une utilisation excessive peut entraîner des risques pour les collaborateurs. Les sollicitations constantes via ces nouveaux modes de communication pendant le temps de travail provoquent une surcharge informationnelle, créent un sentiment d'urgence, de stress, et entraînent en dehors du temps de travail un empiètement grandissant de la vie professionnelle dans la vie privée du collaborateur.

Dans ce contexte, le Groupe Sodiaal s'engage à accompagner les collaborateurs dans le bon usage des outils numériques afin d'améliorer la qualité de vie au travail et réaffirme l'importance de respecter l'équilibre entre vie privée et vie professionnelle en garantissant le droit à la déconnexion pendant le temps de repos.

Il est entendu que les dispositions suivantes n'ont pas toutes vocation à être appliquées :

- Aux cadres dirigeants
- Aux collaborateurs en période d'astreintes
- Aux collaborateurs en déplacement professionnel à l'étranger ou en contact avec l'étranger

1.Droit à la déconnexion pour tous en dehors du temps de travail habituel

Afin de préserver l'équilibre vie professionnelle - vie privée, le Groupe Sodiaal réaffirme que les temps de repos (11h quotidiennes et 35h hebdomadaires), les périodes de congés et de suspension du contrat de travail doivent être respectées par l'ensemble des parties prenantes du Groupe Sodiaal.

A cette fin, le Groupe reconnait un droit à la déconnexion à chaque collaborateur, se traduisant par le droit de ne pas être connecté aux outils numériques professionnels et ne pas être contacté, y compris sur ses outils de communication personnels, pour un motif professionnel en dehors de son temps de travail habituel et pendant ses congés payés, ses temps de repos et ses absences, quelle qu'en soit la nature. Aucun collaborateur ne peut être sanctionné pour avoir fait usage de son droit à la déconnexion.

L'usage des outils numériques en dehors du temps de travail doit être justifié par l'urgence, ou l'importance du sujet traité.

2.Exemplarité des managers et des cadres dirigeants

La hiérarchie s'assurera par son exemplarité du respect du droit à la déconnexion. Le personnel d'encadrement doit particulièrement être attentif à la conciliation entre la sphère professionnelle et la sphère privée des collaborateurs sous leur direction en veillant à ne pas envoyer de courriel en dehors des horaires habituels de travail.

Le Groupe Sodiaal s'engage à ce que le droit à la déconnexion soit un thème obligatoire des entretiens annuels d'évaluation ou, pour les cadres soumis à une convention de forfait en jours, des entretiens sur la charge de travail.

RÈGLES DE BONNES PRATIQUES POUR UNE UTILISATION RAISONNABLE DES OUTILS NUMÉRIQUES PROFESSIONNELS

PENDANT LE TEMPS DE TRAVAIL POUR AMELIORER LA QUALITE DE VIE AU TRAVAIL

- ✓ Pendant les réunions, limiter autant que possible l'usage du PC et du téléphone ;
- ✓ S'interroger sur les fonctions des différents outils de communication en fonction de l'objectif recherché : mails, téléphone, Jabber, My Univers, etc.
- ✓ Privilégier les rencontres physiques à l'envoi de mails afin de favoriser les interactions
- ✓ Veiller à la pertinence des destinataires du mail et à l'utilisation modérée des fonctions « Répondre à tous » et « Copie à »
- ✓ Veiller à la précision de l'objet du mail, cet objet devant permettre au destinataire d'identifier immédiatement le contenu du courriel
- ✓ Eviter l'inscription de la mention « Urgent » et ne pas solliciter de réponse immédiate lorsque ce n'est pas nécessaire ;

EN DEHORS DU TEMPS DE TRAVAIL POUR CONCILIER VIE PROFESSIONNELLE ET VIE PRIVEE

- ✓ Veiller à modérer son utilisation des outils professionnels hors du temps de travail, notamment afin de respecter les temps de repos obligatoires de 11h par jour et 35h par semaine ;
- ✓ S'interroger sur le moment opportun pour envoyer un mail/SMS ou appeler un collaborateur sur son télé- phone professionnel pour éviter de créer un sentiment d'urgence ;
- ✓ Privilégier les envois différés lors de la rédaction d'un mail en dehors des horaires de travail ;
- ✓ Paramétrer le « gestionnaire d'absence au bureau » sur la messagerie électronique et indiquer les coordonnées d'une personne à joindre en cas d'urgence ;
- ✓ Alerter sa hiérarchie en cas de débordements récurrents ;
- ✓ Mentionner dans les mails « si vous recevez ce mes- sage en dehors de vos horaires habituels de travail vous n'êtes pas tenu d'y répondre immédiatement ».
- ✓ Veiller à l'envoi de mails neutres, clairs et concis.

VIII

REGLEMENT D'UTILISATION DES RESSOURCES INFORMATIQUES ET NUMERIQUES

1.Engagement du Groupe en matière de sécurité de l'information

Les présentes dispositions visent à préserver le système informatique du Groupe Sodiaal, dans le respect des obligations légales et règlementaires en vigueur.

Conscient des risques pesant sur la poursuite de son activité en cas d'atteinte à son système d'information (paralysie sur plusieurs semaines), le groupe Sodiaal déploie des efforts significatifs pour atténuer ces actes de malveillance tant externes qu'internes.

Les attaques informatiques se composent de plusieurs phases :

1. Intrusion
2. Prise de contrôle
3. Impacts

Nos usages informatiques peuvent complexifier une intrusion dans nos systèmes, ci-après des exemples de réflexes à intégrer à notre quotidien :

1. Se méfier des mails, au moindre doute effectuer un signalement auprès de MyDSI
2. Refuser de communiquer son mot de passe/de partager son compte
3. Ne rien connecter au réseau (ordinateur, serveur, clef USB, téléphone, disque dur, etc.) sauf fourniture ou autorisation explicite par MyDSI
4. Maintenir vos systèmes/applications à jour et anticiper leur obsolescence
5. Partager vos documents via les plateformes Sodiaal (OneDrive, SharePoint, Teams)

Il est rappelé que chaque utilisateur (collaborateur interne ou externe (CDI, CDD, prestataires intervenants externes, stagiaires, intérimaires, etc.) est directement responsable de l'usage des moyens d'information et de communication auxquels il a accès. Il est chargé, à son niveau, de contribuer à la sécurité générale.

2.Rôle et responsabilités des utilisateurs de ressources informatiques et numériques

L'utilisation des ressources informatiques et numériques est destinée aux besoins de l'activité professionnelle des collaborateurs.
À ce titre, ces ressources peuvent être supprimées, suspendues ou restreintes, notamment en volume (durée de connexion, taille de la messagerie, bande passante disponible, fichiers des pièces jointes, quota d'espace disque, etc.) individuellement ou collectivement quand cela est nécessaire et notamment pour le maintien de la bonne marche et l'intégrité de ressources de l'entreprise.

Les utilisateurs s'engagent à :

> Respecter les lois et règlements en vigueur ; sont notamment prohibées

1. les tentatives d'intrusion de façon illicite sur un système,
2. l'accès aux ressources auxquelles il n'est pas habilité,
3. la consultation
4. la diffusion d'idéologies politiques, raciales ou religieuses, ou qui sont de nature à porter atteinte à l'ordre public, aux bonnes mœurs, à la dignité, à l'honneur ou à la vie privée des personnes.

> Avoir une utilisation non abusive des outils informatiques et numériques auxquels ils ont accès.

Est qualifiée de non abusive une utilisation s'inscrivant dans le cadre des nécessités de la vie courante et familiale, restant raisonnable et raisonné et conforme au présent règlement et règlement intérieur.

Lors d'un usage personnel, l'utilisateur assume la pleine et entière responsabilité et toutes les conséquences juridiques et financières éventuelles.

> Respecter les mesures de sécurité relatives aux ressources informatiques et numériques.

> Respecter le matériel, logiciels et outils mis à leurs dispositions ainsi que les notes techniques et notices d'utilisation relatives à leur mise en œuvre.

> Respecter la confidentialité des données échangées et traitées.

> Informer dans les plus brefs délais de tout dysfonctionnement ou utilisation frauduleuse des outils informatiques et téléphoniques ainsi que de toutes pertes et vols.

> D'aucune façon conduire à la mise en cause de l'image de l'entreprise.

> D'aucune façon gêner ou limiter l'usage professionnel de ces ressources, leur maintenance ou leur sécurité.

> D'aucune façon gêner ou retarder la désactivation des accès d'un collaborateur ou prestataire sortant.

> Ne pas introduire sur le réseau d'équipement non fourni par la Direction des Systèmes d'Information sauf autorisation explicite et formelle.

> Ne pas utiliser les ressources mises à leur disposition pour des activités lucratives ou ludiques.

A. GESTION DES ACCÈS AUX SYSTÈMES

Identifiants :

Les utilisateurs sont responsables de l'utilisation qu'ils font des outils informatiques et téléphoniques du Groupe.
Une identification unique (login et mot de passe) et personnelle est confiée à chaque utilisateur. Cette restriction vise à identifier toute personne utilisant un ordinateur. Cette identification lui permet, à chaque connexion, l'attribution de droits et privilèges propres sur les ressources du système dont il a besoin pour son activité.
L'utilisateur est donc personnellement responsable de l'utilisation qui peut en être faite et ne doit en aucun cas la communiquer.
Ces opérations sont automatiquement tracées à différents niveaux dans les journaux des applications. Ces journaux sont stockés par l'entreprise dans les conditions recommandées par la CNIL.
L'entreprise peut utiliser ces traces comme preuve des agissements du collaborateur et, en

cas d'utilisation pouvant constituer une nuisance, elles peuvent être utilisées pour en établir la preuve.

Nul n'a par ailleurs le droit d'usurper l'identité d'autrui ou d'agir de façon anonyme.
De même, les titulaires de comptes ou de dispositifs de contrôles d'accès sont responsables des opérations effectuées depuis leurs comptes ou sous le couvert des dispositifs de contrôle d'accès qui leur sont attribués.

De façon générale, les utilisateurs doivent prendre toute mesure pour empêcher les accès frauduleux aux outils informatiques et téléphoniques et, à ce titre, ils doivent notamment :

- ✓ Anticiper le départ des collaborateurs ou prestataires rattachés afin de fluidifier la gestion des départs (« Checkout »).
- ✓ Veiller à la confidentialité des comptes utilisateurs qui leur sont attribués.
- ✓ Ne pas prêter, vendre ou céder les comptes utilisateurs, codes ou dispositifs de contrôle d'accès ou d'en faire bénéficier un tiers.
- ✓ Se déconnecter après la fin de leur période de travail sur le réseau ou lorsqu'ils s'absentent.
- ✓ Informer le responsable informatique de toute tentative d'accès frauduleux ou tout dysfonctionnement suspect.
- ✓ S'assurer que les fichiers qu'ils jugent confidentiels ou classés confidentiels ne sont pas accessibles à des tiers non autorisés.
- ✓ S'assurer que leur PC soit mis en mode verrouillage lors d'absences partielles dans la journée, et que le câble de sécurité est fixé pour les PC portables.

Ces identifiants seront verrouillés après le départ du collaborateur (un mécanisme comparable régit le départ des prestataires, tout responsable de partenaire doit être acteur de cette gestion).

Il est également précisé que l'accès de l'utilisateur aux ressources informatiques ou numériques pourra être suspendu, limité ou réexaminé pour des raisons de sécurité, notamment :

> Lors de la cessation de son activité professionnelle au sein de son service ou de l'entreprise (changement de services, mutation, etc.)
> Dans certains cas de cessation temporaire de l'activité professionnelle (congé maladie, congé maternité, etc.)
> Dès lors qu'un usage illicite ou abusif (manquements au présent règlement, etc.) sera suspecté ou démontré

Accès à distance (via VPN) :

Le Groupe Sodiaal met à disposition des utilisateurs nomades un accès dit VPN permettant de travailler sur le réseau d'entreprise à partir de son ordinateur professionnel à l'extérieur de l'entreprise et connecté à Internet. Ces configurations nécessitent une vigilance particulière :

> **La connexion VPN est obligatoire** dès lors que l'utilisateur utilise un réseau public (gare, hall d'hôtel, aéroport, etc.) afin de sécuriser ses communications.
La déconnexion du VPN est obligatoire dès que l'utilisateur quitte le poste.
Le mot de passe ne doit jamais être divulgué.

Spécificités liées au nomadisme :

Seul l'utilisateur autorisé peut connecter un outil de nomadisme au réseau d'entreprise.
Aucun ordinateur ou outil de nomadisme non confié ou agréé par l'Entreprise ne doit être connecté au réseau d'entreprise sans l'autorisation explicite du RSSI.
Tout outil de nomadisme agréé par l'Entreprise pourra être soumis à tout contrôle de sécurité ponctuel ou permanent organisé par le RSSI.
À ce titre le titulaire de l'outil de nomadisme concerné décharge l'Entreprise de toute responsabilité quant à toute conséquence préjudiciable liée à ces contrôles (effacement de données, dysfonctionnement, etc.).

B. RÈGLES DE BON USAGE DES RESSOURCES MIS À DISPOSITION

Généralités :

L'utilisation des matériels mis à disposition est soumise à l'autorisation préalable du supérieur hiérarchique, et peut être retirée à tout moment en cas de non-respect du code de conduite Sodiaal.

L'utilisateur s'engage à n'utiliser cet équipement que dans le cadre professionnel. Il apportera un soin particulier à sa sécurité physique, en particulier dans les véhicules (température, vol) et dans les lieux publics.

L'usage personnel du matériel informatique qui lui est confié est toléré par la Direction dans la mesure où cette utilisation ne perturbe pas l'activité professionnelle de l'entreprise et ne génère pas un surcoût significatif (et à titre exceptionnel). En cas d'abus, la société peut être amenée à effectuer des contrôles.

Toutefois, il est rappelé que pour garantir la sécurité des systèmes, seul un administrateur est autorisé à introduire de nouveaux matériels et logiciels. À ce titre, sont interdits sauf autorisation explicite des services informatiques :

✗ Le téléchargement, l'installation et l'utilisation de logiciels.

✗ L'introduction sur le réseau d'équipements (ordinateur, téléphone, tablette, etc.) non fournis par la Direction des Systèmes d'Information.

Le collaborateur devra informer immédiatement la société en cas de dysfonctionnement, de vol* ou de blocage du matériel informatique.

** Par ailleurs, tout vol de matériel doit faire l'objet d'une plainte déposée à la gendarmerie ou à la police nationale du lieu concerné. Elle sera transmise au gestionnaire du parc informatique ainsi qu'au Délégué à la Protection des Données (DPD/DPO du Groupe : Annabel Francony-Legros annabe.legros@sodiaal.fr / 01 44 10 90 71).*

En cas de contact ou de séjour prolongé à l'étranger hors Union Européenne, l'utilisateur prendra contact avec son correspondant téléphonie afin d'adapter au mieux la tarification.

Respect des droits de propriété intellectuelle :

Il est formellement interdit de copier des logiciels pour quelque usage que ce soit. Les logiciels mis en œuvre à l'Entreprise doivent tous être utilisés et exploités conformément à leur licence d'utilisation et sous réserve des autorisations nécessaires.

Il en est de même pour toutes œuvres telles que photographies, images, bases de données, œuvres audiovisuelles et musicales, textes, etc. protégés par les droits d'auteur. L'Utilisateur ne doit pas, en particulier, utiliser les Ressources mises à sa disposition par l'Entreprise pour porter atteinte aux droits de propriété intellectuelle et en particulier aux droits d'auteur (Téléchargement illicite ou mise en partage non autorisé d'œuvres protégées par le droit d'auteur, etc.).

Spécificités liées à la messagerie électronique :

La messagerie électronique est mise à disposition par l'entreprise pour les échanges professionnels. Les données véhiculées par les flux de messages peuvent être conservées dans les conditions recommandées par la CNIL à des fins de contrôle.

Chaque utilisateur doit prendre conscience qu'un message envoyé par Internet peut potentiellement :

- Revêtir un caractère malveillant (phishing, fraude, etc.)
- Être intercepté, même illégalement, et lu par n'importe qui.

Un objet de messagerie (messages, rendez-vous, carnet d'adresses, tâches, etc.) stocké dans la messagerie électronique par un collaborateur peut avoir un caractère privé, notamment en cas de synchronisation avec un téléphone mobile.

Il appartient au collaborateur d'identifier les objets qui lui sont personnels en donnant la valeur « Privé » dans le choix en liste « Critère de Diffusion » du menu « Propriété » de l'objet.

Un usage privé raisonnable, notamment en nombre et en volume, est toléré dans le cadre des nécessités de la vie courante et familiale, à condition que l'utilisation du courrier électronique n'affecte ni le trafic normal des messages professionnels ni ne perturbe l'activité professionnelle de l'utilisateur. Il appartient au collaborateur d'informer ses correspondants privés afin qu'ils assurent en objet de leurs mails l'identification explicite du caractère privé de leur message.

Le contenu de ceux étant explicitement signalés comme étant de nature privée ne pourront ainsi pas être accédé par l'entreprise sauf autorisation expresse de l'utilisateur, mais un contrôle statistique pourra cependant être effectué afin d'en évaluer l'éventuelle sensibilité ou dangerosité pour l'entreprise et son réseau.
À défaut d'une telle identification, les messages sont présumés être professionnels.

Dans l'utilisation de sa messagerie professionnelle, l'utilisateur veillera à :

- ✗ Rester vigilant au quotidien face aux messages frauduleux ou malveillant (phishing) de quelque nature qu'il soit (demande d'information confidentielle type mot de passe, pièce-jointe piégée, fraude aux virements, etc.) et à notifier son responsable ainsi que le service informatique en cas de doute ou d'action(s) réalisée(s) par inadvertance.
- ✗ Ne pas diffuser d'informations hors de l'entreprise sur l'activité professionnelle, la mission, les projets, les relations au sein du Groupe, ou toute information confidentielle qui pourrait être utilisée par un tiers à des fins d'intelligence économique ou malveillantes.
- ✗ Ne pas participer à des chaînes de courrier électronique.
- ✗ Ne pas dénigrer ou tenir de propos diffamatoire à l'égard de l'entreprise, de ses concurrents ou de quiconque
- ✗ Ne pas communiquer de façon offensante sur la race, le sexe, la religion, les opinions politiques, les origines sociales, l'âge ou le handicap, d'un tiers.
- ✗ Ne pas véhiculer de contenu illicite (pornographie, pédophilie et tous comportements dégradants).
- ✗ Proscrire tout harcèlement sexuel ou moral.
- ✗ S'interdire toute action susceptible d'engager la responsabilité civile ou pénale de l'entreprise.

Spécificités liées à la navigation Internet d'entreprise :

Les utilisateurs doivent faire usage des services d'Internet dans le respect des principes généraux et des règles propres aux divers sites ainsi que dans le respect de la législation en vigueur.
L'utilisation ponctuelle d'Internet à des fins privées est tolérée dans les limites raisonnables à condition que la navigation n'entrave pas l'accès professionnel et ne perturbe pas l'activité professionnelle.

Il est de la responsabilité pénale et éthique de la société d'interdire la consultation de tout site légalement prohibé, notamment à caractère pornographique, pédophile, d'incitation à la haine raciale, révisionniste, etc.

C'est pourquoi un dispositif de filtrage de sites non autorisés (sites diffusant des produits à caractère pornographiques, pédophiles, incitation à la haine raciale, révisionniste, etc.) est administré par le service informatique.

Aucun système ne garantissant un filtre total, un dispositif complémentaire permet l'analyse détaillée des traces de navigation sur Internet. Ces traces sont stockées selon la durée légale en vigueur et analysées périodiquement.

Par ailleurs, les utilisateurs veilleront à ne pas utiliser l'Internet de l'entreprise ou l'adresse e-mail d'entreprise aux fins de :

- ✗ Participation à des forums non professionnels et/ou réseaux sociaux.
- ✗ Création de pages Web personnelles.
- ✗ Exercice d'une activité commerciale personnelle ou d'un travail clandestin.
- ✗ Tentative de violation d'accès des systèmes informatiques.
- ✗ Activités illégales ou contraires aux règles internes.

- ✗ Dénigrement ou propos diffamatoire à l'égard de l'entreprise, de ses concurrents ou de quiconque.
- ✗ Jeux ou agissements visant à obtenir des profits ou gains personnels.
- ✗ Communication offensante portant sur la race, le sexe, la religion, les opinions politiques, les origines sociales, l'âge ou le handicap.
- ✗ Le harcèlement sexuel ou moral
- ✗ Toute action susceptible d'engager la responsabilité de l'entreprise.
- ✗ La pédophilie, la pornographie, l'incitation à la haine raciale, de propos révisionnistes, etc.)

Spécificités liées aux espaces de stockage/partage communs ou individuels :

Par principe, tout espace de stockage/partage de données est mis à disposition par l'entreprise avec vocation de stocker exclusivement des informations professionnelles. Des données privées peuvent de façon exceptionnelle être stockées sur un espace individuel, dès lors que l'espace disque utilisé pour ces données est limité et que ces données sont regroupées dans un dossier nommé « Données personnelles ». En l'absence de cette nomination explicite, ces données pourront être considérées comme étant la propriété de l'entreprise, et donc consultables.

L'espace réseau partagé ne peut en revanche en aucun cas contenir de données autre que professionnelles.

La Direction des Systèmes d'Information se réserve le droit d'exiger la suppression de telles données des réseaux partagés si leur propriétaire peut être identifié, ou à défaut de les supprimer.

3.Rôle et responsabilités des administrateurs

Une Charte d'administration informatique vient en complément de la Charte utilisateur et s'applique à l'ensemble des utilisateurs du Groupe et plus spécifiquement à ceux disposant du statut d'administrateur.

Elle a pour objectif de :

- **De permettre d'éviter toute forme d'abus de l'usage des outils informatiques et constitue un document opposable de référence au sein de Sodiaal.**
- **De préciser les droits et devoirs de l'Administrateur dans l'exercice de sa fonction ou de son activité professionnelle.**

A. GENERALITES

Les administrateurs ont pour mission d'assurer le fonctionnement normal et la sécurité des réseaux et systèmes.

Par leurs fonctions mêmes et par dérogation, ils sont les seuls à avoir accès à des informations personnelles relatives aux utilisateurs (messagerie, historique des sites visités, fichiers « logs » ou de journalisation, etc.), y compris celles qui sont enregistrées sur le disque dur du poste de travail (fichiers temporaires, cookies…).

B. ACCÈS AUX DONNÉES PERSONNELLES DES UTILISATEURS PAR LES ADMINISTRATEURS INFORMATIQUES

L'accès aux données enregistrées par les collaborateurs dans leur environnement informatique — qui sont parfois de nature personnelle — ne peut être justifié que dans les cas où le bon fonctionnement des systèmes informatiques ne pourrait être assuré par d'autres moyens moins intrusifs.

De même, les administrateurs de réseaux et systèmes ne doivent pas divulguer des informations qu'ils auraient été amenés à connaître dans le cadre de leurs fonctions, et en particulier lorsque celles-ci sont couvertes par le secret des correspondances ou relèvent de la vie privée des utilisateurs et ne mettent en cause ni le bon fonctionnement technique des applications, ni leur sécurité, ni l'intérêt de l'entreprise. Ils ne sauraient non plus être contraints de le faire, sauf disposition législative particulière en ce sens.

C. L'UTILISATION DES LOGICIELS DE PRISE DE MAIN A DISTANCE

Les logiciels de prise de main à distance peuvent notamment permettre aux gestionnaires techniques d'accéder à distance à l'ensemble des données de n'importe quel poste de travail, à des fins de maintenance informatique.

Dans l'hypothèse d'un recours à ces outils à des fins de maintenance informatique par un administrateur technique, leur utilisation doit s'entourer de précautions afin de garantir la transparence dans leur emploi et la confidentialité des données auxquelles le gestionnaire technique accédera par ce moyen, dans la stricte limite de ses besoins.

> L'information préalable et le recueil de l'accord de l'utilisateur pour « Autoriser la main » à l'administrateur informatique avant l'intervention sur son poste sont impératifs. À titre d'illustration, l'accord peut être donné par simple validation d'un message d'information apparaissant sur son écran.

✗ L'utilisation des outils de télémaintenance ou de prise de main à distance à des fins de contrôle, par l'employeur, de l'activité de ses collaborateurs sur leur poste informatique est

interdite, car elle n'est ni conforme au principe de proportionnalité ni respectueuse du principe de finalité posé par la loi « informatique et libertés ».

D. CONTINUITE D'ACTIVITE

Lorsque la continuité du service l'exige, les administrateurs peuvent être amenés à prendre les mesures nécessaires afin d'accéder aux ressources mises à disposition de l'Utilisateur absent ou empêché, par exemple pour établir ou rétablir des délégations d'accès ou mettre en place les gestionnaires d'absence adéquats.
L'administrateur auquel est donné l'accès à ces ressources est informé qu'il doit respecter le secret de la correspondance privée et qu'il lui est interdit de prendre connaissance d'éventuels contenus personnels, sous peine de voir sa responsabilité engagée.
L'utilisateur absent est informé au préalable de la nature de l'intervention hors les cas où cela est impossible (absence non prévue).
Afin que ce type de procédure reste tout à fait exceptionnel, il est rappelé l'importance de travailler et de stocker les fichiers sur les espaces partagés afin de faciliter l'accès des fichiers professionnels aux personnes habilitées.
La suppression ou tentative de suppression par l'utilisateur de toute information utile à l'activité de l'entreprise pourra être considérée comme fautive. Par ailleurs, en cas de départ de l'entreprise, les fichiers ou messages à caractère privé qui n'auraient pas été supprimés par l'utilisateur pourront l'être par l'Entreprise, les autres seront réputés appartenir à l'entreprise et conservés comme tel.

4.Contrôle et traçabilité

À des fins de sécurité et de vérification du bon accès et usages des Ressources informatiques, numériques, ainsi que du bon fonctionnement du Système d'information, la Direction des Systèmes d'information met en place des systèmes de Filtrage et de contrôle (pare-feu, systèmes de contrôle des accès, etc.).
Ces systèmes peuvent être mis en œuvre pour contrôler tout message électronique entrant ou sortant (contrôle antiviral, contrôle antispam, contrôle de la taille, liste des destinataires, etc.) et également pour bloquer, notamment sur la base d'une liste de mots clefs, les messages, échanges informatiques ou les accès à des sites non autorisés.
Ils enregistrent les différentes traces d'activité des Ressources, à des fins de sécurité des Systèmes d'information.

Dans le respect des principes de transparence et de proportionnalité, l'Utilisateur est informé que les traces suivantes sont conservées :

> liste des contenus ou services auxquels l'Utilisateur a eu accès sur l'Internet ou l'Intranet ;
> de façon générale, liste des paramètres techniques de gestion des accès/connexion ou tentative d'accès/connexion à tout réseau de communication interne ou externe à partir des ressources (réseau téléphonique, Internet, réseaux internes, etc.) critiques, taille et type des fichiers accédés, etc. ;
> liste des paramètres techniques de gestion des services de Messagerie électronique (identification du compte Utilisateur, coordonnées du destinataire, date et heure, etc.).

À des fins statistiques relatives aux connexions et échanges réalisés, des contrôles portant

notamment sur la volumétrie des connexions à des sites Internet ou sur l'utilisation de la messagerie pourront être réalisés par le RSSI.
Pourront ainsi être mis en place des contrôles a posteriori portant notamment sur la volumétrie des connexions à des sites Internet ou de l'utilisation de la messagerie : relevé des sites les plus visités, des comptes d'Utilisateur ayant généré le plus de requêtes (hits), relevé — pour ceux-ci — des durées de connexion et des sites les plus fréquentés, etc.

✗ L'Utilisateur ne devra en aucun cas empêcher ou gêner le fonctionnement normal de ces moyens de contrôle.

Au besoin, et en fonction du résultat des contrôles opérés, certaines ressources (sites non professionnels visités depuis le réseau de l'Entreprise, etc.) pourront être restreintes voire, interdites par la Direction des Systèmes d'information sans préavis, ni information.

L'Utilisateur est informé que des contrôles individualisés pourront être diligentés par le RSSI, suite à un dysfonctionnement des Ressources, d'une alerte de sécurité (prévention de la fuite de données ou de la violation de données à caractère personnel, etc.) et également en cas de suspicion d'un usage non conforme de ces Ressources, sous réserve du respect des dispositions applicables au secret des correspondances privées.
Dans ce cadre, les constatations matérielles ont pour but de relever les diverses circonstances qui éclaireront la Direction générale, sur l'éventuelle réalisation d'un incident et sur son origine, afin de prendre toutes les mesures, appropriées, le cas échéant en mettant en œuvre les procédures disciplinaires et le cas échéant judiciaires.

Tout manquement aux dispositions du code de conduite pourra faire l'objet d'une sanction disciplinaire et/ou procédure pénale (pour le personnel intérimaire ou extérieur, les procédures disciplinaires relèveront de l'entreprise d'appartenance).

IX
L'ALERTE ÉTHIQUE

PARLONS-EN ENSEMBLE

Chacun d'entre nous, quelle que soit sa position hiérarchique ou son rôle, a le droit de s'exprimer au sujet des situations préoccupantes auxquelles il est confronté et de signaler des faits ou des situations de violation de la loi ou préjudiciable à l'intérêt général, de façon juste, honnête et professionnelle.

La loi du 21 mars 2022 complète les dispositions de la loi du 9 décembre 2016 (dite Loi Sapin) concernant la protection des lanceurs d'alertes (lien vers la loi).
Elle accorde une protection plus complète aux lanceurs d'alertes, définis comme toute personne qui signale sans contrepartie, des informations portant notamment sur un crime, un délit, une infraction quelle qu'en soit la nature.

La loi précise que les lanceurs d'alertes ainsi que leur entourage ne peuvent pas faire l'objet de représailles ou de sanctions telles que notamment : suspension, mise à pied, non- renouvellement de contrat, refus de promotion ainsi que plus largement toutes mesures disciplinaires ou discriminatoires.

Le groupe Sodiaal a mis en place un dispositif d'alerte qui offre aux collaborateurs internes, externes et occasionnels, un moyen alternatif au recours hiérarchique ou à la Direction du Contrôle Interne et de la Conformité, afin de signaler des faits ou des situations de non-conformité.

La procédure d'alerte mise en place au sein du Groupe Sodiaal est conforme aux dispositions de la loi de protection des lanceurs d'alertes. Elle permet le recueil de tout signalement ou révélation réalisés de manière désintéressée et de bonne foi : d'un crime ou délit ; d'une violation grave et manifeste d'un engagement international régulièrement ratifié ou approuvé par la France ; d'une violation grave et manifeste d'un acte unilatéral d'une organisation internationale pris sur le fondement d'un engagement international régulièrement ratifié ou approuvé par la France ; d'une violation grave et manifeste de la loi ou du règlement ; d'une menace ou d'un préjudice grave pour l'intérêt général dont le lanceur d'alerte a eu personnellement connaissance ; relatifs aux obligations définies par les règlements européens et par le code monétaire ou financier ou le règlement général de l'Autorité des marchés financiers, et dont la surveillance est assurée par l'Autorité des marchés financiers ou l'Autorité de contrôle prudentiel et de résolution ; relatifs à l'existence de conduites ou de situations contraires au code de conduite de la société, concernant des faits de corruption ou de trafic d'influence.

COMMENT ALERTER ?

> Téléphone alerte : 0800 94 16 50

> Adresse mail alerte : conformite@groupesodiaal.fr

LA PROTECTION DU LANCEUR D'ALERTE

Conformément à la loi, le groupe Sodiaal s'engage à protéger ses collaborateurs, auteurs d'une alerte via ce dispositif, contre toutes représailles, telles que précisées par l'article 10-1-1 de la loi du 21 mars 2022, dès lors qu'ils agissent de bonne foi.

Cependant, s'il est démontré que le dispositif d'alerte est utilisé dans le but de nuire à autrui, le responsable pourra être sanctionné ou sera susceptible de faire l'objet de poursuites judiciaires.

LA CONFIDENTIALITÉ

Toute situation ou tout fait remonté dans le cadre de ce dispositif d'alerte professionnelle sera traité de façon impartiale et en toute confidentialité. Le dispositif garantit que les éléments de nature à identifier le lanceur d'alerte ne pourront être divulgués qu'avec le consentement de ce dernier. Les données à caractère personnel relatives à tout signalement seront conservées dans le respect des dispositions du règlement du 27 avril 2016 concernant la protection des données personnelles.

Date de la mise à jour du code de conduite : août 2022.