



DÉONTOLOGIE

Votre code de conduite

Les engagements et règles de déontologie présentés dans ce code de conduite s'appliquent à tout collaborateur exerçant ses activités au sein de SOFIAP et toute personne agissant, ou réalisant des opérations au nom et pour le compte de SOFIAP.



Les engagements et règles de Déontologie présentés dans ce code de conduite s'appliquent à tout collaborateur exerçant ses activités au sein de SOFIAP et tout collaborateur de SOFIAP agissant, ou réalisant des opérations au nom et pour le compte de SOFIAP.



SOFIAP, née en 1921 pour faciliter l'accès à la propriété des cheminots, ambitionne aujourd'hui de devenir le premier partenaire des entreprises engagées dans des politiques RSE en développant son offre de prêts immobiliers bonifiés et de crédits à la consommation.

Si notre cœur de métier est le même depuis plus de 100 ans, nos manières de travailler doivent s'adapter au monde d'aujourd'hui, agile, phygital, avec des clients de plus en plus exigeants en termes d'expertise et de réactivité.

Notre adossement au Groupe La Banque Postale nous conforte, je me suis personnellement engagé auprès de nos actionnaires à développer des offres de prêts avec un grand niveau d'expertise et d'assistance pour nos clients entreprises et leurs collaborateurs.

Le code de conduite de SOFIAP est une de nos boussoles. Les règles de déontologie individuelles et collectives qui y sont édictées, combinées avec les valeurs que nous portons, viennent renforcer la confiance établie avec nos parties prenantes, et notamment nos clients, partenaires et collaborateurs.

En ce début d'année 2024, la mise à jour du code de conduite accompagne les profondes transformations de notre entreprise, engagée pour faire progresser l'accès à la propriété par le prêt subventionné par les entreprises et accompagner les aidants en permettant à nos aînés à bien vivre chez soi.

À tous les niveaux de responsabilité de notre entreprise, je compte sur chacune et chacun d'entre nous pour le respecter et pour que ses principes guident nos actions.

Je compte sur vous.

Bien à vous.

Mickael LE NEZET
Président du directoire de SOFIAP

Table des matières

Avant-propos	4
Nos valeurs	4
Notre code de conduite	4
1. Règles de bonne conduite communes aux collaborateurs	6
1.1. Règles de déontologie personnelle	6
1.2. Dispositif et règles de prévention et de gestion des conflits d'intérêts	9
1.3. Politique cadeaux et invitations	17
1.4. Respect de la confidentialité et du secret professionnel.....	20
1.5. Respect des règles afférentes au traitement de données à caractère personnel	20
2. Règles de bonne conduite vis-à-vis des clients	22
2.1. Une politique commerciale qui priorise l'intérêt des clients.....	22
2.2. Une relation professionnelle et objective qui concourt à la protection des intérêts des clients	23
2.3. Une démarche citoyenne de protection de la clientèle.....	24
3. Règles de bonne conduite vis-à-vis des marchés	27
3.1. Respect des règles en matière de concurrence.....	27
3.2. Respect des engagements citoyens	28
4. Règles de conduite applicables à la lutte contre la corruption et au trafic d'influence	29
4.1. Engagement de SOFIAP	29
4.2. Définitions	29
4.3. Illustrations	32
4.4. Situations à risques et comportements attendus de la part des collaborateurs	33
4.5. Prévention des actes de corruption	35
4.6. Sanctions.....	35
5. Lutte contre le blanchiment et le financement du terrorisme	36
5.1. Connaissance clients (KYC).....	36
5.2. Vigilance constante des opérations	36
5.3. Lutte contre le financement du terrorisme et respect des embargos	37
5.4. Coopération avec les autorités de surveillance et de régulation.....	37
6. Politique fiscale	38
6.1. Recherche d'une maîtrise de la charge fiscale.....	38
6.2. Maîtrise du risque fiscal	38
Annexes	39
Annexe 1 : Charte utilisateur des moyens informatiques	57
1.1. Préambule.....	57
1.2. Droits et devoirs des utilisateurs	58
1.3. Contrôles et collecte d'informations	64
1.4. Sanctions.....	64
Annexe 2 : Charte administrateur des moyens informatiques	65
1.5. Préambule.....	65
1.6. Administrateurs informatiques.....	65
1.7. Traçabilité et Contrôle	68
1.8. Sanctions.....	68

Avant-propos

SOFIAP est l'entreprise de tous et accueille avec respect et considération toute personne, quelle que soit sa situation.

Nos valeurs

Les règles de bonne conduite édictées par le code s'inscrivent pleinement dans les valeurs définies par SOFIAP :

- **accessibilité** : être là où les clients ont besoin de nos services et quand ils en ont besoin, en adaptant nos modes de distribution de l'ensemble de nos produits aux nouveaux usages. Lutter contre l'exclusion, en proposant une offre accessible et responsable,
- **équité** : s'adapter à la diversité des situations et des demandes et y répondre avec une égale attention et une égale efficacité,
- **considération** : traiter les clients et les collaborateurs avec l'attention et le respect qu'ils attendent,
- **proximité** : être disponible pour tous les clients dans chaque lieu et chaque site, en s'adaptant à leurs spécificités,
- **ouverture** : porter un regard neuf sur la société, être en permanence à l'écoute de ses parties prenantes pour capter leurs évolutions et leur proposer des solutions toujours adaptées,
- **sens du service** : se mettre au service du client, à travers un mode de relation fondé sur l'écoute et le professionnalisme.

Ces valeurs conduisent à :

- **favoriser l'accessibilité, la proximité et le développement territorial,**
- **lutter contre l'exclusion, en proposant une offre accessible et responsable,**
- **conforter la relation de confiance avec les clients.**

Ces valeurs fondent également les valeurs éthiques sur lesquelles les activités de SOFIAP et de ses collaborateurs s'appuient :

- **intégrité, loyauté et transparence vis-à-vis des clients, des marchés, des prestataires, des tiers, et de l'entreprise,**
- **professionnalisme et objectivité dans les relations d'affaires,**
- **considération et respect des clients et des collaborateurs,**
- **attention apportée à l'impact environnemental et social des activités.**

Notre code de conduite

Le code de conduite est la déclaration des valeurs et des missions qui guident SOFIAP, ainsi que ses collaborateurs dans leur activité du quotidien. Il expose les règles fixées par le Groupe. Celles-ci définissent un comportement déontologique et des pratiques responsables.

Ces règles constituent une obligation professionnelle. Nul ne peut se prévaloir de l'ignorance des règles de déontologie. Le non-respect des dispositions du présent code engage la responsabilité personnelle du collaborateur et l'expose à des sanctions disciplinaires, civiles, voire pénales selon la réglementation applicable.

Le code de conduite manifeste aussi l'engagement du Directoire dans une démarche de prévention et de détection des faits de corruption et de lutte contre l'utilisation de ses services aux fins de blanchiment d'argent ou à des fins criminelles.

Il contribue à la relation de confiance qui unit SOFIAP à ses clients et partenaires, à préserver l'entreprise du risque de réputation et du risque réglementaire. Le code de conduite rappelle les politiques de SOFIAP et prévoit des règles de déontologie, destinées à être appliquées par chacun des collaborateurs exerçant ses activités au sein de SOFIAP et à toute personne agissant, ou réalisant des opérations en son nom et pour son compte.

Le code de conduite est annexé au règlement intérieur, remis aux nouveaux entrants et disponible sur l'Intranet de SOFIAP.

Le code de conduite est un document à caractère public complété par des « politiques » qui précisent les règles et engagements sur des sujets spécifiques. Les politiques suivantes sont abordées au sein du code de conduite¹ :

Le code de conduite traduit les valeurs historiques et éthiques de SOFIAP. Il marque aussi l'engagement de l'instance dirigeante dans une démarche de prévention et de détection des faits de corruption ou d'utilisation du système financier à des fins de blanchiment d'argent ou de financement du terrorisme.

- Politique de prévention et de gestion des conflits d'intérêts,
- Politique de lutte contre la corruption,
- Politique cadeaux et invitations,
- Politique de responsabilité sociétale d'entreprise (RSE) au travers de celle de La Banque Postale,
- Charte pour une représentation d'intérêts responsable du Groupe La Banque Postale,
- Politique d'achats responsables,
- Politique de maîtrise des risques,
- Politique de sécurité des systèmes d'information,
- Politique de rémunération,
- Politique thématique de sécurité « maîtrise des informations et des usages »,
- Politique d'évaluation des tiers.

En cas de soupçon d'une violation ou d'un contournement des règles et principes édictés dans ce code (y compris les documents auxquels il fait renvoi) ou de la loi, le dispositif d'alerte peut être actionné en utilisant l'adresse suivante : www.alerte-ethique.laposte.fr.

(*) liste non exhaustive des politiques de SOFIAP et/ou du Groupe La Banque Postale

1. Règles de bonne conduite communes aux collaborateurs

Chaque collaborateur veille à garantir la primauté des intérêts des clients, dans le respect des exigences réglementaires et des procédures en vigueur au sein de SOFIAP.

Par ailleurs, les collaborateurs s'engagent à promouvoir et à respecter les règles de bonne conduite en vigueur au sein de SOFIAP.

Ces règles concernent les comportements attendus vis-à-vis des clients de SOFIAP, des prestataires, et des tiers, mais aussi les bonnes relations que chacun doit entretenir au sein des services.

La déontologie est une discipline qui doit être partagée par tous et notamment relayée par les managers. Elle renvoie à des principes généraux tels que le professionnalisme, l'indépendance de jugement, la confidentialité, la transparence, le respect des règles de marché, qui sont autant de repères dans l'exercice des activités.

1.1. Règles de déontologie personnelle

1.1.1. Respect et considération des personnes

Chacun au sein de SOFIAP, quelles que soient ses responsabilités, doit veiller au respect et à la considération de tous les collaborateurs.

1.1.2. Règles générales de comportement

Les collaborateurs respectent les règles de comportement édictées par le Règlement Intérieur de SOFIAP, et notamment :

- d'une manière générale, il est interdit de porter atteinte au bon ordre, à la discipline, et à la sécurité des biens et des personnes,
- les collaborateurs sont tenus à un devoir de réserve, qui implique l'usage de propos prudents et mesurés, et proscrit l'injure et la grossièreté tant dans les écrits que dans les attitudes. La coopération entre les services et entre les collaborateurs eux-mêmes doit être la règle,
- les collaborateurs doivent s'abstenir de tout agissement fautif, notamment au travers de comportements qui pourraient être assimilés au harcèlement sexuel ou moral, des agissements sexistes ou des violences internes.

En toutes circonstances, chacun doit veiller à adopter un comportement respectueux, responsable et décent dans sa présentation et sa tenue vestimentaire.

1.1.3. Loyauté et intégrité

Tout collaborateur agit avec professionnalisme, diligence et loyauté envers SOFIAP et son personnel, les clients et les différentes parties prenantes. Il doit promouvoir l'intérêt de SOFIAP et des clients en contribuant activement tant à la réalisation de ses objectifs qu'à la coopération entre les différentes activités.

Tout collaborateur doit s'abstenir, sauf autorisation expresse de sa hiérarchie et/ou du déontologue, de prêter son concours à titre onéreux ou gratuit, à des personnes morales ou physiques exerçant une activité associative ou professionnelle concurrente de SOFIAP.

Tout collaborateur agit avec professionnalisme, diligence et loyauté envers la SOFIAP et son personnel, les clients et les différentes parties prenantes.

Par ailleurs, tout collaborateur a une obligation d'informer sans délai sa hiérarchie ou le déontologue de toute situation de nature à engager directement ou indirectement la responsabilité civile ou pénale de SOFIAP.

Plus généralement, tout collaborateur s'engage à respecter l'intégrité du patrimoine de SOFIAP et celui des clients.

1.1.4. Utilisation des ressources et équipements

1.1.4.1. Habilitations et sécurité des systèmes d'information

Dans l'exercice de leur métier, les collaborateurs disposent de pouvoirs, habilitations et droits qu'il convient de respecter et protéger. En aucun cas, ceux-ci ne peuvent être usurpés ou communiqués, toute utilisation des droits d'un autre collaborateur étant formellement interdite.

Les ressources et équipements sont mis à la disposition des collaborateurs pour l'exercice de leurs activités professionnelles. Chaque utilisateur est responsable de la protection des équipements, et ne peut en conséquence modifier ou désactiver les mécanismes de protection.

Dans le cadre de ses activités, tout collaborateur doit respecter la charte utilisateur des moyens informatiques (Annexe 1) et pour les fonctions afférentes la charte administrateur des moyens informatiques (Annexe 2). Ces chartes précisent les règles d'accès et d'utilisations des ressources des systèmes d'information mises à disposition.

En particulier :

- toute connexion à des sites Internet ayant un caractère explicitement indécent ou choquant est strictement interdite, de même que le visionnage ou le téléchargement de données prohibées par la loi,
- une vigilance accrue lors de l'utilisation des messageries électroniques est requise afin que le contenu des messages ne porte pas atteinte à la réputation et sécurité de SOFIAP,
- la confidentialité des informations doit être assurée, aussi bien au sein de SOFIAP qu'à l'occasion d'une utilisation des ressources dans un lieu externe et/ou public,
- les informations professionnelles manipulées par tout utilisateur doivent être classifiées selon leur sensibilité afin d'en assurer leur protection,
- toute information professionnelle (données, documents, fichiers...) de SOFIAP, y compris celle(s) produite(s) par l'utilisateur dans le cadre de son activité, est la propriété de SOFIAP. Tout transfert d'information en dehors du système d'information de SOFIAP est interdit sauf dérogation dûment validée en utilisant les outils adaptés mis à disposition par SOFIAP,
- les règles à respecter en matière de transfert d'information en dehors de l'entreprise sont définies dans la politique thématique de sécurité « maîtrise des informations et des usages » accessible à tous les utilisateurs sur l'Intranet,
- un dispositif de surveillance des fuites de données (Data Loss Protection) est déployé sur le système d'information de SOFIAP afin de détecter les potentiels incidents dans ce domaine,
- l'usage à titre privé des ressources et équipements mis à disposition des collaborateurs est toléré dès lors qu'il reste raisonnable. Les données personnelles doivent être enregistrées dans des répertoires appropriés, et leur consultation est strictement encadrée,
- la modification de la configuration des équipements est interdite hors accord ou intervention des services informatiques. De même, aucun logiciel non référencé ne peut être installé.

Il est du devoir de chaque utilisateur d'alerter, selon les procédures en vigueur, en cas de suspicion ou de constatation d'événements pouvant porter atteinte à la sécurité des systèmes d'information de SOFIAP.

1.1.4.2 Intelligence artificielle

L'intelligence artificielle (IA) représente tout outil utilisé par une machine afin de reproduire des comportements liés aux humains, tels que le raisonnement, la planification et la créativité.

Tout système mettant en œuvre des mécanismes proches de celui d'un raisonnement humain peut ainsi être qualifié d'intelligence artificielle.

Parmi ces intelligences artificielles, on trouve l'intelligence artificielle générative (IA générative) capable de produire automatiquement du contenu original (texte, image, audio, vidéo, etc.) à partir de modèles entraînés sur de grandes quantités de données. Bien que puissants, ces systèmes peuvent présenter des risques en matière de fuite de données, de confidentialité, de sécurité et de fausse information notamment.

Ainsi, l'accès et l'utilisation de l'IA générative sont en principe interdits sauf dérogation dûment justifiée et validée. Le cas échéant, son utilisation doit être encadrée et contrôlée en respectant les lignes directrices suivantes :

- ne jamais partager de données professionnelles d'une classification supérieure à C0,
- vérifier la qualité des informations fournies par l'IA générative,
- ne pas prendre de décision sur la seule base des informations proposées par l'IA.

1.1.5. Médias sociaux, espaces d'échange et communication externe

SOFIAP est présente sur les réseaux sociaux et espaces d'échange, et propose des contenus adaptés à son positionnement et à ses valeurs.

Dans le cadre de la stratégie digitale de SOFIAP, des collaborateurs participent à ces échanges qui visent à instaurer une relation privilégiée avec les clients et à leur offrir de nouveaux modes de contact. En toute circonstance, il convient de veiller aux règles professionnelles et de bonne conduite, notamment en matière d'information et de confidentialité.

Plus globalement, toute participation des collaborateurs de SOFIAP sur des forums ou groupes de discussion ou à des médias dits « sociaux » doit se faire dans le respect des bonnes pratiques existantes et, en tout état de cause, dans le respect de la législation et des bonnes mœurs, en prenant garde de ne pas porter atteinte à l'image de SOFIAP.

Seuls les dirigeants effectifs et les personnes spécialement habilitées sont autorisés à prendre la parole au nom de SOFIAP. Tous les autres collaborateurs ne prennent la parole qu'à titre personnel. À ce titre, aucun collaborateur ne peut conseiller ou promouvoir des produits et services vendus (prospection interdite) par SOFIAP, hors partage de publications officielles. Il est aussi interdit aux collaborateurs de répondre à la place du service client.

Les collaborateurs doivent aussi veiller à respecter la réglementation au sujet des droits d'image, marque etc...

La communication externe et les relations avec les autorités de tutelle, étatiques et la presse sont assurées et centralisées par des personnes dûment habilitées par le Directoire de SOFIAP.

1.1.6. Harcèlement au travail et agissements sexistes

SOFIAP réaffirme que le respect mutuel, la dignité et la confiance sont des valeurs qui doivent être placées au cœur de la relation de travail et garanties en toutes circonstances.

À ce titre, l'entreprise a mis en place un dispositif de traitement des situations de souffrance au travail, incluant le harcèlement moral, sexuel, les agissements sexistes, mais également tout dysfonctionnement engendrant une situation de mal être voire un épuisement professionnel.

Chaque signalement émanant des salariés peut être reçu par le manager, la Direction des Ressources Humaines (DRH), le service de santé au travail, les représentants du personnel, le référent en matière de lutte contre le harcèlement sexuel et les agissements sexistes, ou par le déontologue (directement ou via la plateforme d'alerte).

Le signalement est traité dans les meilleurs délais par la DRH de SOFIAP et fait l'objet d'un examen approfondi. Il est consigné dans un registre dédié, tenu par la DRH.

Dès la réception du signalement et dans un délai de 15 jours, une phase d'écoute est mise en place, au cours de laquelle le salarié et la personne visée par le signalement sont entendus par la DRH.

À l'issue de cette phase d'écoute, la DRH peut, si elle l'estime nécessaire, déclencher une phase d'investigation, comportant la mise en place d'un comité de pilotage paritaire, composé de deux représentants de la DRH, du secrétaire et d'un membre du CSE (comité social et économique).

Cette phase d'investigation permet d'enquêter auprès de tout témoin ou personne pouvant apporter son éclairage sur la situation, afin d'identifier les actions à mettre en place pour y remédier.

La DRH et le CSE, dont le référent en matière de lutte contre le harcèlement sexuel et les agissements sexistes sont chargés d'orienter, informer et accompagner les salariés les sollicitant.

Les collaborateurs sont informés de la réglementation en vigueur, au travers d'actions d'information, de prévention et de sensibilisation.

1.1.7. Lutte contre les discriminations

La diversité est l'une des valeurs historiques de l'entreprise dont le modèle social prône l'égalité des chances au sein même de cette diversité.

Dans ce cadre, aucune personne au sein de SOFIAP ne peut faire l'objet d'une discrimination directe ou indirecte identifiée par la loi, en application de l'article L. 1132-1 du code du travail.

1.1.8. Droit d'alerte

Tout collaborateur exerçant des activités au sein de SOFIAP, personnel agissant ou réalisant des opérations en son nom et pour son compte, ainsi que les personnes intervenant dans un cadre contractuel (prestataire – stagiaire-alternant – intérimaire – sous-traitant – fournisseur et ses collaborateurs) disposent d'un droit d'alerte.

Le dispositif d'alerte permet à tout lanceur d'alerte de questionner le déontologue sur une problématique éthique mais aussi de signaler tout manquement aux valeurs de SOFIAP, les comportements/situations contraires au code de conduite ou les informations portant sur des faits répréhensibles ou contraires à l'intérêt général qui pourraient être préjudiciables à une personne ou à l'entreprise.

Il contribue au respect des engagements éthiques et déontologiques de SOFIAP (dont la lutte contre la corruption) conformément à la loi Sapin II du 9 décembre 2016.

Il répond également aux exigences relatives au devoir de vigilance.

Le terme alerte désigne tout signalement ou divulgation transmis de bonne foi et sans contrepartie financière directe, d'informations portant sur un crime, un délit, une menace ou un préjudice pour l'intérêt général, une violation ou une tentative de dissimulation d'une violation 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, du droit de l'Union européenne, de la loi ou du règlement.

Le terme alerte désigne également le signalement de comportements ou de situations contraires au code de conduite.

À cet effet, SOFIAP a fait le choix de recourir à un prestataire de service pour recueillir les alertes et permettre au lanceur d'alerte de bénéficier d'une sécurisation des échanges, conformément à la réglementation applicable en matière de protection des données à caractère personnel.

Les alertes doivent être déposées à l'adresse suivante : www.alerte-ethique.laposte.fr.

Toute personne ayant exercé un droit d'alerte bénéficie du dispositif de protection des lanceurs d'alerte (confidentialité, anonymat, absence de représailles, non-discrimination etc...) mis en place par SOFIAP.

[Une procédure spécifiquement dédiée à ce sujet est disponible sur le site Intranet de SOFIAP.](#) Les déontologues de La Poste et de La Banque Postale, le référent déontologue de SOFIAP peuvent être conduits à partager le traitement des alertes dont ils ont la connaissance.

1.2. Dispositif et règles de prévention et de gestion des conflits d'intérêts

1.2.1. Cadre réglementaire

La politique de prévention et de gestion des conflits d'intérêts s'inscrit dans le cadre d'un ensemble de textes législatifs et réglementaires applicables à SOFIAP du fait de ses activités et de son organisation.

La réglementation européenne impose aux établissements et entreprises soumis au contrôle de la Banque Centrale Européenne (BCE) ou de l'autorité de contrôle prudentiel et de résolution (ACPR) d'établir et de maintenir une politique efficace de gestion des conflits d'intérêts.

En France, l'arrêté du 3 novembre 2014 modifié le 25 février 2021 relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement et l'article 522-2 du code des assurances exigent l'application par SOFIAP de procédures pour prévenir et gérer les conflits d'intérêts.

Par ailleurs, la directive européenne des assurances (directive DDA) exige que l'intermédiaire ou l'entreprise d'assurance qui exerce des activités de distribution de produits d'assurance maintienne et applique des dispositifs organisationnels et

administratifs efficaces en vue de prendre toutes les mesures raisonnables destinées à empêcher que des conflits d'intérêts ne portent atteinte aux intérêts de ses clients.

Les orientations de l'autorité bancaire européenne (ABE) sur les politiques et les pratiques de rémunération liées à la vente et à la fourniture de produits et de services de banque de détail (EBA- GL-2016-06) imposent des obligations de déclaration et des orientations sur les politiques et les pratiques de rémunération.

Les orientations de l'ABE relatives à la gouvernance interne (EBA/GL/2017/12) exigent des politiques en matière de conflits d'intérêts et des procédures d'alerte.

1.2.2. Définitions, périmètre et objectifs

1.2.2.1. Définitions

Une situation de **[conflit d'intérêts]** existe lorsqu'un intérêt particulier d'ordre matériel, professionnel, commercial, financier ou **personnel** vient concurrencer l'intérêt du client, de SOFIAP, des marchés ou de tout autre **[tiers]**.

Définition de **[l'intérêt personnel]** : il peut être matériel (patrimonial, financier, commercial...) ou moral (intérêts politiques, religieux...). Il peut être direct ou indirect, c'est-à-dire concerner le **[collaborateur]** ou son **entourage**.

On entend par **[entourage]** tout parent ou membre de la famille (y compris concubinage, pacs...) toute relation amicale ou habituelle (membre d'un club, d'une association...) ainsi que toute personne physique ou morale avec laquelle le **[collaborateur]** a, ou a eu, des relations d'affaires ou politiques.

On entend par **[tiers]** toute personne ou entité ayant conclu un engagement contractuel avec SOFIAP (prestataires, fournisseurs, partenaires ...), y compris les **collaborateurs**.

Le terme **[collaborateur]** utilisé au sein de cette politique désigne tout collaborateur exerçant ses activités au sein de SOFIAP quel que soit son niveau hiérarchique occupé au sein de l'entreprise, et tout collaborateur de La Banque Postale agissant ou réalisant des opérations au nom et pour le compte de SOFIAP.

1.2.2.2. Périmètre

La Politique s'applique à l'ensemble des collaborateurs et instances dirigeantes de SOFIAP.

Les activités couvertes par la politique comprennent les activités de financement et d'intermédiaire d'assurance.

Il est à noter que les obligations de prévention et de gestion des conflits d'intérêts dédiées aux produits d'assurance et produits bancaires, issues de la Directive Distribution Assurance (DDA) s'inscrivent dans le cadre de la Politique.

1.2.2.3. Objectif

Les activités de financement et d'assurance peuvent par nature être source de conflits d'intérêts. Les conflits d'intérêts non maîtrisés peuvent conduire à une perte de revenus, à porter atteinte à l'image de SOFIAP, ou aux intérêts des clients et à donner lieu à des recours juridiques et à une sanction disciplinaire et pécuniaire des superviseurs et régulateurs à l'encontre de SOFIAP.

La politique de prévention et de gestion des conflits d'intérêts de SOFIAP a pour objectif la maîtrise de ces situations à risques.

Les situations de conflits d'intérêts sont inhérentes à la vie de l'entreprise. Au cours de son activité, un collaborateur peut être influencé par des intérêts extérieurs. Ces situations ne sont pas nécessairement répréhensibles ou nocives pour l'entreprise. Elles nécessitent toutefois d'être encadrées par des dispositions de nature à les identifier, les prévenir et les gérer.

Certaines situations de conflits d'intérêts portant atteinte aux intérêts de l'entreprise peuvent être pénalement sanctionnées en cas d'atteinte aux intérêts de l'entreprise, comme l'abus de biens sociaux¹ ou la prise illégale d'intérêts².

Des sanctions administratives peuvent également être prononcées à l'encontre de SOFIAP.

La Politique décrit le dispositif de SOFIAP et les procédures à suivre afin **d'identifier, évaluer, gérer ou atténuer les conflits d'intérêts** avérés et potentiels qui se posent entre :

- SOFIAP vis-à-vis de ses collaborateurs (ou les collaborateurs vis-à-vis de SOFIAP),
- SOFIAP et ses collaborateurs vis-à-vis des clients (y compris les clients-collaborateurs),
- SOFIAP et ses collaborateurs vis-à-vis des tiers (y compris les entreprises partenaires au titre du prêts bonifiés/subventionnés par ces dernières au profit de leurs salariés).

¹ Pour un dirigeant, c'est le fait de « faire de leur pouvoir, ou des biens de la société un usage qu'ils savent contraire aux intérêts de la société, à des fins personnelles ou pour favoriser une autre société ou entreprise dans laquelle ils sont intéressés directement ou indirectement ».

² C'est le fait « pour un élu, une personne dépositaire de l'autorité publique ou chargée d'une mission de service public, de prendre, recevoir ou conserver un intérêt quelconque dont il a la charge d'assurer la surveillance ou l'administration ».

1.2.3. Cadre mis en place par SOFIAP

1.2.3.1. L'engagement des dirigeants

L'engagement en matière de gestion et de prévention des conflits d'intérêts est porté au plus haut niveau de SOFIAP : la politique fait l'objet d'une validation par le conseil de surveillance de SOFIAP. Pratiquement, elle est mise en œuvre sous la responsabilité du référent déontologue de SOFIAP.

1.2.3.2. Cadre normatif de SOFIAP

1.2.3.2.1. Cadre normatif général

Le cadre normatif défini pour SOFIAP qui s'impose à tous les collaborateurs est constitué :

- du code de conduite,
- de la politique de prévention et de gestion des conflits d'intérêts,
- de la politique de lutte contre la corruption fixant les règles et les comportements à adopter ou à proscrire.

Les éléments décrits ci-dessus sont communiqués aux collaborateurs dès leur intégration dans l'entreprise (le code de conduite étant annexé au règlement intérieur qui est remis à l'embauche).

La vigilance de tous les collaborateurs est appelée sur l'identification de toute situation relevant d'un conflit d'intérêts, qu'il soit potentiel ou avéré.

Le code de conduite est mis à jour régulièrement, notamment en cas d'évolution législative ou réglementaire significative, avec au minimum une revue annuelle.

1.2.3.2.2. Cadre normatif spécifique aux produits d'assurance et produits bancaires

En application de la réglementation européenne directive des assurances (DDA), SOFIAP dispose de procédures dédiées visant la prévention des conflits d'intérêts pour les produits d'assurance et produits bancaires.

Ces procédures traitent de :

- l'identification,
- la prévention,
- et le traitement des conflits d'intérêts susceptibles de nuire à la qualité des services rendus aux clients.

1.2.4. Identification des conflits d'intérêts

Les conflits d'intérêts peuvent survenir lors des relations que SOFIAP et ses collaborateurs initient avec les clients ou différents tiers, mais aussi en interne à l'occasion de la réalisation des activités au sein des services.

Eu égard aux risques énoncés au paragraphe 1.2.2 « définitions, périmètre et objectif », l'identification des conflits d'intérêts, avérés ou potentiels, au sein des structures/entités ou départements de SOFIAP est un préalable nécessaire à leur prévention.

1.2.4.1. Typologie des conflits d'intérêts

L'analyse d'une situation permettant de déterminer l'existence de conflits d'intérêts au sein de l'entreprise résulte de différents facteurs qui doivent être pris en compte dans la démarche d'identification :

- la forme plus ou moins avérée du conflit d'intérêts (cf. § 1.2.4.1.2),
- l'évolution dans le temps de la situation de conflit d'intérêts. Par exemple : survenance d'une évolution professionnelle (nouvelles fonctions) ou personnelle (nouvelle activité de bénévolat) de la personne concernée, existence d'une nouvelle relation d'affaires (un nouveau client...),
- la diversité des activités de l'entreprise,
- la diversité des intérêts (personnels, professionnels) qui peuvent intervenir. Par exemple : relations avec le Groupe La Banque Postale ou SNCF, responsabilités associatives du collaborateur, l'entourage du collaborateur.

1.2.4.1.1. Conflits d'intérêts potentiels

Constitue un risque de conflit d'Intérêts **potentiel**, la situation qui laisse apparaître un conflit d'intérêts présumé dont la réalisation n'est pas concrétisée.

Le risque de conflit d'intérêts non encore identifié peut survenir, temporairement ou durablement, face à une situation nouvelle.

Toute situation nouvelle doit être appréciée au regard du risque de conflit d'intérêts et évaluée par les responsables désignés (cf. § 1.2.5 : dispositif de prévention et § 1.2.6 : gestion des conflits d'intérêts de la politique).

Les conflits d'intérêts potentiels sont recensés dans la cartographie des conflits d'intérêts.

1.2.4.1.2. Les conflits d'intérêts avérés (réels ou apparents)

Constitue un risque de conflit d'intérêts **avéré** toute situation dans laquelle le conflit d'intérêts potentiel s'est réalisé. Il doit faire l'objet d'une déclaration (cf. § 1.2.6 : gestion des conflits d'intérêts).

Toute situation de conflit d'intérêts avéré doit être prise en compte par les collaborateurs concernés, que leur caractère soit **durable ou temporaire**.

1.2.4.2. Identification des conflits d'intérêts

Pour illustrer un conflit d'intérêts potentiel ou avéré, SOFIAP ou les collaborateurs doivent prendre en compte les exemples suivants (liste non exhaustive) :

1.2.4.2.1. Conflits d'intérêts dans la relation avec les clients

- Réaliser un gain financier ou éviter une perte financière aux dépens du client,
- Posséder un intérêt différent de celui du client dans le résultat d'un service fourni au client ou d'une transaction exécutée pour celui-ci, par exemple : proposer des produits aux clients en raison d'un intérêt personnel particulier, tel un commissionnement commercial plus incitatif (dans tous les cas, l'intérêt du client doit être priorisé),
- Être incité pour des raisons financières ou autres, à favoriser les intérêts d'un autre client ou groupe de clients par rapport à ceux du client concerné,
- Posséder un intérêt dans une entreprise ou une structure exerçant la même activité professionnelle (ou en concurrence) avec SOFIAP,
- Recevoir, d'une personne autre que le client, une rémunération en relation avec le service fourni au client, sous forme d'un avantage monétaire ou non monétaire,
- Interférer dans le traitement d'un dossier de crédit concernant un membre de son entourage.

1.2.4.2.2. Conflits d'intérêts dans la relation avec les Tiers

- Inciter fortement à l'entrée en relation d'affaires avec une société où un membre de son entourage occupe un poste important,
- Faire embaucher/être impliqué dans la décision d'embauche, en interne comme en externe, d'un membre de son entourage, en passant outre le processus RH,
- Faire embaucher/être impliqué dans la décision d'embauche par un fournisseur ou prestataire, d'un membre de son entourage,
- Favoriser un cabinet de recrutement au motif que l'on connaît bien les dirigeants,
- Être dans un rapport d'encadrement, de subordination ou de contrôle avec un membre de son entourage,
- Détenir un intérêt financier direct ou indirect ou un intérêt personnel dans une entreprise en lien commercial actuel ou possible (prospect), ou en concurrence avec son entité,
- Exercer une activité professionnelle autre (bénévole ou rémunérée) en concurrence avec celles de SOFIAP,
- Passer outre les processus de l'entreprise³ (ex : un appel d'offres) dans la sélection d'un fournisseur/ prestataire pour favoriser une entrée en relation d'affaires (par exemple : imposer un tiers parce qu'une entrée en relation d'affaires est attendue en retour).

1.2.4.2.3. Conflits d'intérêts dans les produits d'assurance et produits bancaires

- Entretenir des liens capitalistiques étroits avec une entité (entreprise d'assurance, société de gestion, entreprise d'investissement, filiale, partenaire), incitant à recommander à un client un produit conçu ou distribué par cette entité, alors qu'un autre produit qui correspondrait mieux à ses exigences et besoins pourrait lui être proposé.
- Mettre en œuvre un dispositif de rémunération, d'objectifs de vente et/ou d'évaluation de la performance incitant les conseillers à recommander un produit particulier à un client alors qu'ils pourraient proposer un autre produit qui correspondrait mieux aux exigences et besoins du client.
- Utiliser des informations confidentielles obtenues d'un client au détriment d'un autre client.

³ La politique d'achats responsables de SOFIAP vise notamment à garantir l'indépendance des différents acteurs intervenant dans le processus achat, en particulier les prescripteurs, acheteurs et décideurs, et les prémunir de toute situation de conflits d'intérêts.

1.2.4.2.4. Conflits d'intérêts dans les situations de cumul de mandats

- Existence d'un cumul de mandats (professionnels, politiques) : par exemple, siéger au conseil d'administration d'un partenaire, d'un concurrent, d'un fournisseur ou d'un client de SOFIAP. L'existence de cumul de mandats impose, en soi, d'observer une vigilance particulière afin de bien prendre en compte l'ensemble des risques potentiels (le conflit d'intérêts, mais également le risque d'atteinte à la réputation) que présente ce type de situation,
- Intervenir dans un processus de négociation ou décisionnel, tels les appels d'offres, les liens d'affaires avec une association, pour lequel le collaborateur ou son entourage exercerait des fonctions,
- Utiliser son mandat d'élu pour favoriser SOFIAP par exemple dans l'octroi de marchés publics.

1.2.4.3. Cartographie des conflits d'intérêts

Les cartographies de risques de conflit d'intérêts ont pour objet d'identifier les conflits d'intérêts potentiels ou avérés.

SOFIAP dispose d'une cartographie, établie par le référent déontologie :

- des conflits d'intérêt de nature personnelle,
- des conflits d'intérêt au titre de ses activités de financement et d'assurance.

Ces cartographies sont mises à jour de manière continue (création d'une nouvelle activité ou d'un produit innovant, nouveaux mandats externes d'un collaborateur, acquisition / cession d'une participation) et au minimum une fois par an pour tenir compte notamment des évolutions des processus métiers et pour réévaluer les dispositifs associés à la prévention et à la détection des conflits d'intérêts.

La revue des cartographies de conflits d'intérêts est réalisée formellement une fois par an afin de s'assurer de la bonne prise en compte des évolutions des processus métiers et des nouvelles situations (potentielles ou avérées) de conflits d'intérêts.

Elle s'appuie sur :

- l'exploitation du registre des conflits d'intérêts, qu'il soit tenu manuellement ou via un outil électronique mis à disposition des collaborateurs (cf. § 1.2.6.1),
- l'analyse des questionnaires de déclaration des conflits d'intérêts des dirigeants (cf. § 1.2.5.6),
- les alertes ou signalements reçus par le déontologue dans l'année écoulée.

Le cas échéant, la cartographie est complétée par les nouvelles situations identifiées et par les dispositifs de maîtrise associés (existants ou à renforcer), de nature à prévenir, détecter ou gérer le conflit d'intérêts.

La revue annuelle de la cartographie vise également à réévaluer l'ensemble des dispositifs de maîtrise des risques, de façon à s'assurer de leur pertinence et de leur efficacité.

1.2.5. Dispositifs de prévention des conflits d'intérêts

1.2.5.1. Dispositions générales participant à une prévention des conflits d'intérêts

1.2.5.1.1. Formation et sensibilisation

- Les collaborateurs sont formés à travers une formation dédiée à la déontologie, comportant un chapitre relatif aux conflits d'intérêts,
- Des actions de sensibilisation des collaborateurs sont réalisées par la direction en charge de la déontologie ou les managers, au regard de l'exposition aux conflits d'intérêts spécifiques à chaque métier,
- Un référent déontologie est désigné au sein de SOFIAP dans le cadre de la filière déontologie,
- Des comités déontologie réunissant les référents sont tenus régulièrement et animés par le déontologue du Groupe permettant de définir et valider les actions prioritaires, d'échanger sur des thématiques communes et de partager les bonnes pratiques notamment sur la thématique des conflits d'intérêts.

1.2.5.1.2. Dispositions en matière de cadeaux et invitations

Dans le respect des principes fondamentaux définis par la politique cadeaux et invitations en vigueur au sein de SOFIAP (cf. § 1.3) l'acceptation de cadeaux et invitations répond à un questionnement strict que chaque collaborateur doit mener avant de répondre favorablement à la sollicitation.

1.2.5.1.3. Obligation d'agir de manière honnête loyale et professionnelle

Les collaborateurs comme les dirigeants de SOFIAP ont un devoir de loyauté vis-à-vis de SOFIAP et veillent à ne pas induire une situation susceptible de générer un conflit d'intérêts.

Pour ce faire et agir au mieux des intérêts du client, SOFIAP a mis en place des dispositifs qui visent à :

- bien connaître les clients et leurs besoins,

- informer les clients qui doivent disposer de l'ensemble des informations leur permettant de comprendre les caractéristiques des services et produits proposés,
- fournir des produits adaptés,
- documenter et tracer le conseil apporté aux clients,
- surveiller les situations de fragilité des clients.

Par ailleurs, un dirigeant s'interdit de souscrire des produits de SOFIAP à des conditions différentes de celles offertes au public (sauf cas d'exception prévus pour les collaborateurs de SOFIAP – Prêt au personnel).

1.2.5.2. Dispositions organisationnelles participant à une prévention des conflits d'intérêts

Les directions, départements de SOFIAP peuvent, du fait de leurs interactions, systèmes d'information, de la complémentarité de certaines activités au sein de SOFIAP, de l'existence de clients communs et/ou concurrents, être confrontés à des situations de conflits d'Intérêts.

Ces entités définissent des mesures d'organisation pour exercer leur activité sans générer de conflits d'Intérêts.

1.2.5.2.1. Protection des informations confidentielles

Au-delà des obligations de secret professionnel, la prévention des conflits d'intérêts passe en premier lieu par une protection des informations confidentielles.

L'ensemble des informations auxquelles tout collaborateur a accès à l'occasion de l'exercice de sa fonction doit être considéré comme confidentiel, même au sein de sa direction ou département.

En toute circonstance, SOFIAP ou l'un de ses collaborateurs doit pouvoir agir en toute indépendance, dans l'intérêt des clients et de SOFIAP.

Les directions de SOFIAP définissent les fonctions et la séparation des professions et activités (barrière à l'information) au sein de leur périmètre d'activité afin de prévenir les conflits d'intérêts.

Par principe, la circulation des informations confidentielles doit être limitée aux seuls personnels ayant besoin de les connaître (principe du « Besoin d'en connaître » ou « Need to know »).

Les collaborateurs de SOFIAP respectent les dispositions relatives à la protection des informations établies par SOFIAP et notamment les mesures prévues en fonction du niveau de classification des données.

1.2.5.2.2. Politique de rémunération des forces de vente

La politique de rémunération des forces de vente commerciales repose sur des principes de performances individuelle et collective, dont les modalités de calcul prennent en compte des critères de conformité de l'activité commerciale. La rémunération à l'acte de vente est interdite.

Il appartient donc aux managers, aux forces de vente commerciales, aux lignes d'animation, de support et de contrôle de s'assurer de l'absence d'incitation à proposer un produit ou service qui ne répondrait pas à l'intérêt du client.

1.2.5.3. Règles de prévention des conflits d'intérêts vis-à-vis des clients et des clients - collaborateurs

Les règles définies ci-après ne limitent pas la vigilance que le collaborateur doit s'imposer s'il s'estime exposé à une situation de conflit d'intérêts dans le cadre de son activité.

1.2.5.3.1. Règles de prévention vis-à-vis des clients

- Tout collaborateur ne peut recevoir pour lui-même ou pour un membre de son entourage, une procuration ou un mandat d'un client, sauf si ce dernier est une personne entretenant avec le collaborateur un lien préexistant de nature familiale, fiscale ou légale,
- Tout collaborateur ne peut bénéficier, ou faire bénéficier un membre de son entourage (famille, concubinage, Pacs...), directement ou indirectement, sous quelque forme que ce soit, de prêts, dons legs, et plus généralement de toute libéralité ou transfert patrimonial de la part d'un client, sauf s'il s'agit d'une personne entretenant avec le collaborateur un lien préexistant de nature familiale, fiscale ou légale,
- Tout collaborateur ne peut se faire porter, ou faire porter un membre de son entourage, comme bénéficiaire d'un contrat de quelque nature que ce soit, souscrit par un client, sauf s'il s'agit d'une personne entretenant avec le collaborateur un lien préexistant de nature familiale, fiscale ou légale. Toute captation d'héritage, sous quelque forme que ce soit, est strictement interdite.

1.2.5.3.2. Règles de prévention vis-à-vis des clients-collaborateurs

- Un collaborateur ne peut réaliser, à partir des installations professionnelles de l'entreprise (applicatifs/ applications), des opérations ou transactions pour son propre compte ou pour un compte sur lequel il détient un mandat (dans le

respect des règles relatives aux relations avec les clients). Ce collaborateur ne peut pas être, simultanément et pour son propre compte, à la fois collaborateur et client,

- Un collaborateur ne doit pas intervenir dans la gestion du prêt d'un client lorsque des liens hiérarchiques et fonctionnels existent entre les deux personnes,
- Les opérations et transactions des clients-collaborateurs doivent être traitées par un collaborateur n'ayant pas de lien hiérarchique ou fonctionnel avec le client-collaborateur.

On entend par lien fonctionnel, celui qui existe entre :

- des collaborateurs situés au même niveau et travaillant dans un même domaine, et donc sans lien de subordination existant entre eux,
- un collaborateur ayant une relation de management avec d'autres collaborateurs (rattachement fonctionnel), qui ne serait pas fondée sur la hiérarchie mais sur l'expertise et ou la filière.

Ainsi, le client et le collaborateur ne doivent pas avoir de liens ou d'interactions dans le cadre professionnel, qu'ils soient hiérarchiques ou non.

1.2.5.4. Règles de prévention vis-à-vis des tiers

- Tout collaborateur doit s'interdire d'intervenir dans un processus de négociation ou décisionnel, tels les appels d'offres, les liens d'affaires avec une entreprise, pour lequel le collaborateur ou son entourage sont susceptibles de détenir un intérêt personnel,
- Cette interdiction concerne aussi les collaborateurs qui détiendraient des mandats électifs ou exerceraient des fonctions dans le domaine associatif. En toute circonstance, l'indépendance et l'objectivité d'analyse et de décision du collaborateur doivent être garanties,
- Dans le cadre de l'exercice de ces mandats électifs ou fonction dans le domaine associatif, ces exigences d'indépendance et d'objectivité sont aussi requises afin que les personnes concernées, par ailleurs collaborateurs, ne favorisent pas indûment les intérêts de SOFIAP ou de l'association,
- Tout collaborateur doit s'interdire de favoriser ou de nuire aux intérêts et droits d'un collaborateur en raison de liens personnels entre ceux-ci,
- Tout collaborateur doit s'interdire d'exercer une activité qui viendrait en concurrence avec celles de SOFIAP.

1.2.5.5. Les règles de prévention vis-à-vis des marchés

- Il est strictement interdit à tout collaborateur de SOFIAP, qui a connaissance d'informations privilégiées dans le cadre son activité, de réaliser, ou de tenter de réaliser, des opérations sur les marchés d'instruments financiers, directement ou par personne interposée, ou de permettre à un tiers, sciemment ou non, de réaliser de telles opérations en lui communiquant ces informations ou en recommandant à celui-ci d'effectuer cette opération. Ces infractions constituent un délit d'initié.
- La mise en place des « barrières à l'information » précisées dans Le règlement général de l'AMF (article 315-15) doit être recherchée afin de prévenir l'apparition de situation de conflit d'intérêts et se prévenir de la circulation et l'utilisation d'informations privilégiées.

1.2.5.6. Dispositions spécifiques en matière de prévention des conflits d'intérêts des organes de direction

Les dirigeants concernés au titre de ce paragraphe sont les dirigeants effectifs de SOFIAP, c'est-à-dire les membres du Directoire de SOFIAP.

La prévention des conflits d'intérêts des dirigeants est réalisée par les deux dispositifs suivants :

- À la prise de fonctions, la complétude du questionnaire « Fit and Proper » destiné à la BCE,
- Annuellement, la complétude du questionnaire de déclaration et de gestion des conflits d'intérêts des dirigeants « Questionnaire de déclaration et de gestion des situations de conflits d'intérêts des dirigeants effectifs ».

Par ailleurs, s'agissant des mandats, les dirigeants informent le référent déontologue de SOFIAP :

- lors de leur prise de fonction et avant toute prise ou sortie de mandat des mandats éventuellement détenus,
- en cours de mandat, de toute prise de nouveau mandat extérieur à SOFIAP.

Chaque dirigeant effectif de SOFIAP est tenu, pendant toute la durée de son mandat, d'apprécier par lui-même si sa situation est susceptible de générer des conflits d'intérêts et s'il respecte les règles relatives au cumul des mandats.

A cet effet, il complète chaque année, **le questionnaire de déclaration et de gestion des situations de conflits d'intérêts**, qu'il transmet au référent déontologue de SOFIAP.

Si nécessaire en cours d'année et notamment, dès que survient un événement (personnel ou professionnel) susceptible de faire évoluer sa situation (personnelle, professionnelle et/ou financière), il lui appartient de transmettre au référent déontologue de SOFIAP une version mise à jour du questionnaire.

1.2.6. Gestion des conflits d'intérêts

1.2.6.1. Déclaration

Que faut-il déclarer ?

Dès lors qu'il anticipe ou qu'il se trouve dans une situation de conflit d'intérêts potentielle ou, avérée (telles que décrites ci-dessus), tout collaborateur de SOFIAP doit en faire la déclaration.

À qui ?

La déclaration doit être faite auprès du manager et du référent déontologue de SOFIAP.

Il convient de préciser qu'il est toujours possible, à tout moment, de prendre avis auprès du référent déontologue de SOFIAP.

La déclaration est le gage de transparence nécessaire et indispensable pour dissiper le risque relatif au caractère dissimulé (volontairement ou involontairement) du conflit d'intérêts. Elle doit permettre d'éviter des conséquences préjudiciables tant pour le collaborateur que pour SOFIAP.

Plus généralement, il est recommandé à chaque collaborateur, en toute circonstance, de partager ses doutes et interrogations avec sa hiérarchie ou le référent déontologue de SOFIAP.

Cette déclaration, ou cette interrogation peut être faite par un mail adressé à sa hiérarchie et/ou référent déontologue de SOFIAP.

Il est également possible d'utiliser la plateforme sécurisée permettant le dépôt d'une alerte, en garantissant la confidentialité et, le cas échéant, l'anonymat à l'adresse suivante : www.alerte-ethique.laposte.fr, en sélectionnant « Groupe La Banque Postale » puis « SOFIAP ».

Quand ?

Les collaborateurs sont appelés à déclarer les situations (temporaires ou permanentes) susceptibles de constituer un conflit d'intérêts, ou qui pourraient apparaître comme tel, **à leur entrée dans l'entreprise et au fil de leurs évolutions personnelles ou professionnelles.**

Comment ?

Cette déclaration doit prendre un caractère formel et se matérialiser par l'établissement d'une déclaration de conflit d'intérêts qui doit comprendre l'identité du collaborateur et la description de la situation.

Concernant les dirigeants effectifs, cette déclaration fait l'objet d'une procédure spécifique, revue annuellement.

Traitement des déclarations

En cas de conflit d'intérêts avéré, le référent déontologue instruit le dossier en s'appuyant si besoin sur un groupe ad hoc et en coordination, le cas échéant, avec le déontologue du Groupe La Banque Postale. Tout conflit sera documenté et donnera lieu à un avis inscrit dans le registre des conflits d'intérêts tenu par le référent déontologue de SOFIAP.

Registre des déclarations

Le référent déontologue de SOFIAP tient à jour le registre des déclarations qui comporte la liste nominative des conflits d'intérêts qui sont portés à sa connaissance ou qu'ils peuvent être amenés à identifier.

La déclaration des conflits d'intérêts vis-à-vis des clients

Dans certains cas, les mesures internes, telles que décrites ci-dessus ne s'avèrent pas suffisantes, notamment lorsqu'il subsiste un risque de conflit d'intérêts perçu.

Dans une optique de transparence, il peut s'avérer possible de tenir informé le client ou le tiers, voire de refuser l'opération afin de protéger les parties prenantes.

Notamment, en matière d'activités liées aux produits d'assurance ou aux produits bancaires, si le dispositif mis en place pour gérer le conflit d'intérêts ne permet pas d'avoir la certitude raisonnable que le risque de porter atteinte aux intérêts du ou des client(s) ne peut être évité, SOFIAP peut gérer le conflit selon les modalités suivantes :

- les clients sont informés de manière claire et détaillée sur la situation de conflit d'intérêts identifiée, sa nature, ses causes et ses conséquences. Les clients sont dans la mesure du possible informés des mesures prises pour atténuer les

risques que le conflit d'intérêts présente pour eux,

- l'information est communiquée avant la fourniture du produit ou avant l'exécution du service pour que le(s) client(s) puisse(nt) prendre une décision en connaissance de cause,
- dans certaines circonstances, SOFIAP pourra refuser de réaliser l'opération concernée, préalablement ou après l'information du (des) client(s).

1.2.6.2. Mesures managériales

Des mesures managériales peuvent être mises en place. Elles se matérialiseront par des systèmes de contrôle (double signature, validation par un tiers, contrôle hiérarchique, transparence...) ou par des mesures organisationnelles (rattachement différent d'un collaborateur pour la gestion d'un dossier, transfert de fonctions à un autre collaborateur...).

Dans certains cas, le processus même de décision pourra être aménagé : collégialité de décision, arbitrage d'une fonction hiérarchique supérieure, etc.

1.2.6.3. Déport

Le déport consiste en une obligation d'abstention pour le périmètre des missions ou des activités concernées par le conflit d'intérêts.

Le déport est une réponse fiable et efficace à la situation de conflit d'intérêts, notamment lorsqu'il s'agit d'une situation ponctuelle (par exemple, dans le cas de la négociation d'un contrat de prestations avec un fournisseur avec lequel le collaborateur en charge du projet a des liens d'intérêts déclarés).

Le déport est également adapté pour gérer une situation de conflit d'intérêts sur un périmètre restreint de l'activité ou des missions du collaborateur. L'abstention d'intervention du collaborateur sur un processus décisionnaire sera alors permanente, mais cantonnée à un périmètre clairement établi avec son manager ou sa hiérarchie.

Cette mesure ne doit en aucune manière être confondue avec une sanction.

1.3. Politique cadeaux et invitations

1.3.1. Principes fondamentaux relatifs aux cadeaux et invitations

Les règles retenues par SOFIAP en matière de cadeaux et invitations visent à préserver les collaborateurs de situations qui pourraient compromettre leur objectivité et leur indépendance de jugement, ou qui pourraient en donner l'impression à l'extérieur.

Chacun doit veiller à appliquer strictement ces dispositions afin de conserver une posture de droiture dans les actes quotidiens.

Le principe fondamental est de veiller à ce que les cadeaux et invitations susceptibles d'être offerts ou reçus par les collaborateurs s'inscrivent systématiquement dans un contexte professionnel clair et transparent et ne puissent être soupçonnés d'influencer une décision ou le traitement d'un dossier par les collaborateurs.

1.3.2. Définitions

[Un agent public] désigne les agents publics élus ou nommés ainsi que toute personne employée comme agent par une organisation publique internationale, une administration nationale, régionale ou locale, ou par une société directement ou indirectement détenue ou contrôlée par l'Etat.

[Un cadeau] désigne tout avantage matériel (paiement, gratification, présent ou avantage quelconque) offert ou reçu dans le cadre de ses activités professionnelles.

[Une invitation] désigne tout avantage ou service immatériel (événement, divertissement sportif ou culturel, voyage, hébergement, repas, etc.) offert ou reçu dans le cadre de ses activités professionnelles. NB : Y compris les repas d'affaires, les invitations à des colloques, séminaires...

1.3.3. Cadre général

La Politique cadeaux et invitations s'impose à l'ensemble des collaborateurs de SOFIAP, ainsi qu'aux personnels agissant pour son compte sur instruction de leurs employeurs respectifs. Ces règles s'appliquent aussi bien pour les cadeaux et invitations reçus que ceux offerts.

Il convient de noter que SOFIAP a retenu des modalités différentes suivant que le cadeau ou l'invitation est reçu ou offert par un représentant public (cf. § 1.3.4 et 1.3.5).

1.3.3.1. Règles générales

Chaque collaborateur doit s'assurer que la sollicitation dont il fait l'objet ne sera pas de nature à nuire à son indépendance, à fausser son jugement et ses décisions. Ainsi :

- Tout collaborateur de SOFIAP doit par principe refuser tout cadeau ou invitation qui serait de nature disproportionnée par rapport à une manifestation de courtoisie conforme aux usages,
- La perception d'une somme d'argent, ou d'une carte cadeau est interdite,
- Tout cadeau ou invitation sortant du cadre professionnel doit être refusé,
- Tout cadeau ou invitation, quelle qu'en soit la valeur, ne peut être accepté dès lors qu'il pourrait rendre le collaborateur redevable à l'égard du donateur.

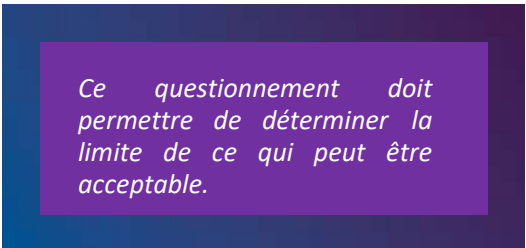
À ce titre, **il est strictement interdit à un collaborateur de recevoir (ou offrir) un cadeau ou une invitation lors de moments stratégiques, par exemple à l'occasion d'appel d'offres, de signature d'accord, de vote...**

- En cas de doute sur la recevabilité d'un cadeau ou invitation, le collaborateur doit solliciter son supérieur hiérarchique et/ou le référent déontologue qui décidera ou non de son acceptation. Cette décision doit être tracée et archivée.
- De même, dans le cas où le refus du cadeau pourrait altérer les relations avec le client, le collaborateur devra interroger sa hiérarchie et la déontologie qui pourront immédiatement décider de remettre le cadeau à une institution charitable choisie par le collaborateur concerné, ou à la Fondation de France, si le déontologue l'estime préférable.
- Les mêmes règles s'appliquent que le cadeau ou l'invitation soit **reçu ou offert**.

1.3.3.2. Questionnement

Dans le respect des principes fondamentaux définis par la Politique cadeaux et invitations en vigueur au sein de SOFIAP, l'acceptation ou l'offre de cadeaux et invitations répond à un questionnement strict que chaque collaborateur doit mener avant de répondre favorablement à la sollicitation.

Ce questionnement doit permettre de déterminer la limite entre ce qui peut être acceptable de ce qui ne l'est pas. En toute circonstance, la transparence et l'indépendance doivent être assurées.



Ce questionnement doit permettre de déterminer la limite de ce qui peut être acceptable.

En pratique, il convient notamment de s'interroger sur les aspects suivants :

- La sollicitation est-elle bien conforme aux législations en vigueur et à la Politique cadeaux et invitations de SOFIAP ?
- La sollicitation s'inscrit-elle dans un cadre essentiellement professionnel et en dehors de tout contexte spécifique : appels d'offre – accord... ?
- La sollicitation est-elle d'une valeur raisonnable, compte tenu des responsabilités de la personne à qui il est accordé et de l'occasion considérée, et susceptible notamment d'une réciprocité ?

1.3.4. Modalités d'information et d'autorisation des cadeaux et invitations

En complément, des règles ont été fixées au regard de la valeur financière du cadeau ou de l'invitation :

- **cadeau ou invitation d'une valeur inférieure à 70 €** : ils peuvent être acceptés (ou offerts) sans autorisation préalable ni obligation de déclaration, s'ils s'inscrivent dans un cadre professionnel et n'enfreignent pas les règles générales,
- **cadeau ou invitation d'une valeur comprise entre 70 € et 150 €** : l'acceptation (ou l'offre) doit faire l'objet d'une autorisation du supérieur hiérarchique,
- **cadeau ou invitation d'une valeur supérieure à 150 €** : l'acceptation (ou l'offre) est soumise à l'autorisation du supérieur hiérarchique et avis du déontologue

Rappel : les cadeaux et invitations sont interdits (y compris les repas d'affaires), quel que soit le montant, en période d'appel d'offres ou lors de moments stratégiques, par exemple à l'occasion de signature d'accord, de vote....

Les cadeaux et invitations refusés d'une valeur supérieure à 70 € doivent également être déclarés.

En pratique :

En cas de doute sur la légitimité du cadeau ou de l'invitation proposé, chaque collaborateur doit solliciter son responsable hiérarchique ou le référent déontologue.

Le collaborateur doit s'assurer d'avoir respecté les obligations déclaratives et, le cas échéant, obtenir l'autorisation de son supérieur hiérarchique, préalablement à l'acceptation ou l'offre du cadeau ou de l'invitation.

Les demandes d'information ou de déclaration sont adressées par mail.

Les documents relatifs aux demandes d'information ou d'autorisation du supérieur hiérarchique doivent être conservés par les personnes concernées et être produites en cas de contrôle.

1.3.5. Règles spécifiques s'appliquant aux relations avec des agents ou représentants publics

Tout cadeau ou invitation, quel que soit son montant, **dès le 1^{er} euro** doit faire l'objet d'une demande d'autorisation préalable auprès du supérieur hiérarchique et d'un avis du référent déontologue⁴. Cela concerne notamment les entreprises publiques avec lesquelles SOFIAP est en relation.

Rappel : Les cadeaux et invitations sont interdits, quel que soit le montant, en période d'appel d'offres (y compris les repas d'affaires).

1.3.6. Illustrations

1^{re} illustration

Une collaboratrice de SOFIAP invite à déjeuner dans un restaurant italien réputé, une de ses collègues, car sa fille postule au sein de sa direction. Le processus de recrutement pour ce poste est en cours. La candidate a été reçue et fait partie des candidats en lice pour le poste.

⁴ Les membres du Directoire de SOFIAP sont tenus à une déclaration au déontologue

Cette invitation ne peut pas être acceptée car il s'agit d'un moment stratégique : le processus de recrutement RH est toujours en cours et l'invitation à déjeuner pourrait influencer le choix final du recrutement.

2^e illustration

Une prestation est en cours de renouvellement au sein d'une direction. Un appel d'offres est en cours et la société de prestation qui délivre actuellement la prestation fait partie de l'appel d'offres. Le prestataire qui preste au sein de la direction ainsi que son manager invitent l'ensemble de l'équipe au restaurant pour les remercier de l'accueil réservé durant leurs années de présence. La valeur du déjeuner est estimée à 500 €.

L'équipe doit refuser l'invitation à déjeuner car il est strictement interdit à un collaborateur de recevoir une invitation à l'occasion d'appel d'offres. En acceptant cette invitation, cela pourrait fausser le jugement des collaborateurs pour le choix du nouveau prestataire le cas échéant.

3^e illustration

Fin décembre, un collaborateur reçoit de la part d'un fournisseur, une caisse de champagne d'une valeur de 250 €. Il n'y a pas d'appel d'offres en cours.

Il n'y a pas d'obstacle à accepter ce cadeau, néanmoins au regard de sa valeur, il devra déclarer le cadeau auprès de son manager par mail et attendre l'autorisation formelle de son manager avant de l'accepter.

1.4. Respect de la confidentialité et du secret professionnel

L'ensemble des informations auxquelles tout collaborateur a accès à l'occasion de l'exercice de sa fonction doit être considéré comme confidentiel.

- Tout collaborateur est donc tenu à une obligation générale et permanente de confidentialité nécessitant de ne pas consulter, utiliser, exploiter, directement ou indirectement, pour son propre compte ou celui d'un tiers, toute information confidentielle ou privilégiée, dont il doit aussi assurer la protection,
- L'obligation de confidentialité ne fait pas obstacle aux communications obligatoires définies par la loi, les règlements, les règles et procédures internes, la hiérarchie directe, les organes de contrôles internes tels l'Audit, la déontologie, l'inspection bancaire, ou les organes de contrôles externes expressément autorisés par SOFIAP,
- Les informations perdent leur caractère confidentiel lorsqu'elles sont publiques, que l'autorité hiérarchique de SOFIAP en a autorisé expressément la publication, ou lorsque la personne, physique ou morale, concernée a donné l'autorisation expresse de divulgation.

Par principe, la circulation des informations confidentielles doit être limitée aux seuls personnels ayant besoin de les connaître pour le bon exercice de leur fonction « **Need to know** ».

Par ailleurs, tout collaborateur de SOFIAP est tenu au secret professionnel qui est une exigence légale, garante de la confiance du client envers SOFIAP. Ainsi :

- Tout collaborateur de SOFIAP, à qui des renseignements confidentiels sont demandés doit, sauf cas de dérogation légale, opposer le secret professionnel aux tiers, que le client soit une personne physique ou morale,
- L'information sur le client doit rester confidentielle aussi bien vis-à-vis de l'extérieur de SOFIAP, que vis-à-vis des collaborateurs de SOFIAP dont les opérations ne sont pas directement concernées par l'information,
- Des dérogations à l'obligation de secret professionnel peuvent être autorisées à l'initiative du client, et au titre des dérogations légales, de l'autorité judiciaire agissant dans le cadre d'une procédure pénale, des autorités bancaires et financières (autorité des marchés financiers, l'autorité du contrôle prudentiel, La Banque de France), des chambres de compensation des marchés réglementés, de TRACFIN, des commissaires aux comptes de sociétés commerciales, de l'administration fiscale,
- En cas de non-respect de cette obligation par le collaborateur, l'article 226-13 du code pénal dispose que la révélation d'une information à caractère secret est punie d'un an d'emprisonnement et de 15 000 euros d'amende.

1.5. Respect des règles afférentes au traitement de données à caractère personnel

La protection des données personnelles concerne de nombreux aspects du travail au quotidien et ne peut être assurée qu'avec la participation active de chacun. Cet impératif se retrouve dès la conception de nouveaux projets, services ou produits, et doit être constant tout au long de la durée de conservation des données en question.

Les collaborateurs doivent ainsi seulement utiliser les données personnelles nécessaires à leur activité et exclusivement dans le but pour lequel elles ont été recueillies. Également, il est nécessaire d'informer de leurs droits les personnes dont les données sont traitées. Il est possible de s'adresser au référent en charge de la protection des données personnelles de SOFIAP afin d'obtenir des conseils. Il est essentiel d'avoir une attention particulière à la sécurité des données comme à leur

confidentialité et de signaler toute violation ou suspicion de violation des informations personnelles conservées.

En revanche, il est **strictement interdit de communiquer des données personnelles** (par exemple en envoyant par mail des fichiers qui en contiennent par facilité), **de créer un fichier de données personnelles, numérique ou papier, sans déclaration préalable auprès du délégué à la protection des données de son entité et sans information des personnes concernées** ; il est également interdit de conserver et d'utiliser des données pour des finalités autres que celles prévues.

Illustration 1

Je travaille au sein d'un service qui est conduit à traiter des données personnelles de clients. Un client souhaite connaître les données personnelles le concernant. Il demande également la destruction de ces données.

Puis-je accéder à la demande de ce client ?

Oui, vous le devez. Chacun a le droit de connaître les données le concernant et de demander leur effacement. La demande de votre client est donc fondée. Vous devez la transmettre, pour traitement, au délégué à la protection des données de SOFIAP qui jugera si celle-ci peut y accéder. Il existe en effet certaines restrictions à l'effacement des données, en particulier si des enquêtes, des instructions civiles ou pénales sont en cours.

Illustration 2

Je traite régulièrement des informations clients au format papier. J'ai l'habitude de laisser mes dossiers clients sur mon bureau le soir pour éviter d'aller les rechercher le lendemain. Mon bureau n'est pas fermé mais mon établissement est sécurisé.

Cette situation comporte-t-elle des risques ?

Oui. La protection des données ne peut être assurée que si vous mettez les dossiers sous clé à votre départ. Dans le cas cité, la sécurisation globale du bâtiment ne remplit pas les exigences réglementaires de protection des données et vous faites porter à SOFIAP un risque en matière de protection des données personnelles de ses clients. Vous devez donc mettre vos dossiers clients sous clé.

2. Règles de bonne conduite vis-à-vis des clients

SOFIAP s'engage à proposer à l'ensemble de ses clientèles une offre de produits et services répondant à leurs besoins, au juste tarif, et dans le respect des réglementations en vigueur.

Pour cela, SOFIAP met en œuvre une politique commerciale responsable qui vise à garantir les intérêts des clients, en accord avec sa politique de responsabilité sociétale d'entreprise (RSE).

Chaque collaborateur doit avoir le souci constant d'agir avec professionnalisme, transparence et objectivité envers les clients, en veillant notamment à dispenser l'information et le conseil attendu le mieux adapté à leurs exigences et besoins, permettant aux clients de décider en toute connaissance.

Chaque collaborateur doit avoir le souci constant d'agir avec professionnalisme, diligence, transparence et objectivité envers les clients.

Cette exigence doit être partagée tout au long des relations que SOFIAP entretient avec ses clients, une vigilance toute particulière devant être maintenue pour détecter toute situation de fragilité et vulnérabilité qui pourrait être préjudiciable aux intérêts des clients.

Chacun, à son niveau de responsabilité, est porteur de cet engagement majeur.

2.1. Une politique commerciale qui priorise l'intérêt des clients

2.1.1. Des produits et services proposés au juste tarif

SOFIAP propose à ses clients une gamme de produits et de services simples, transparents, responsables, adaptés à leurs exigences et besoins, avec des tarifs uniques sur tout le territoire. Une plaquette tarifaire claire et simple est portée à la connaissance de tous les clients, en toute transparence.

Dans ce cadre, SOFIAP s'attache à vérifier de manière régulière l'attractivité de son offre tarifaire.

2.1.2. Des informations communiquées exactes, claires et non trompeuses

SOFIAP est attentive à fournir aux clients toutes les informations utiles leur permettant de comprendre les caractéristiques essentielles des produits, de pouvoir les comparer afin de décider en toute connaissance de cause et dans leur intérêt.

Aussi, SOFIAP s'est organisée afin de s'assurer de la conformité des produits avant toute mise en marché, en particulier que les **informations communiquées aux clients sont exactes, claires, non trompeuses et qu'elles seront bien comprises**, que les processus de vente prennent en compte les textes juridiques et réglementaires, dans l'intérêt des clients et de SOFIAP.

Par ailleurs, il est aussi vérifié que l'engagement de SOFIAP de proposer une offre responsable de produits et services prenant bien en compte les **critères extra-financiers**, tels les critères **éthiques** en matière de conseil, de **transparence**, de simplicité, est bien respecté.

2.1.3. Une politique de rémunération des forces de vente responsable

Le modèle de management commercial met en avant l'esprit d'équipe au service de la performance collective.

En cohérence avec un objectif de développement commercial sain et durable et toujours soucieuse de prioriser les intérêts des clients, la politique de rémunération des forces de ventes commerciales repose sur des principes de performances individuelle et collective, dont les modalités de calcul prennent en compte des critères de conformité de l'activité commerciale.

Par ailleurs, la politique de prévention et de gestion des conflits d'intérêts de SOFIAP conduit à s'assurer de l'absence d'incitation à proposer un produit ou service qui ne serait pas dans l'intérêt des clients.

Il appartient aux managers, aux forces de vente commerciales, aux lignes d'animation, de support et de contrôle de veiller au respect de ces orientations et d'en favoriser la réalisation.

2.2. Une relation professionnelle et objective qui concourt à la protection des intérêts des clients

2.2.1. Bien connaître les clients et leurs besoins

L'entrée en relation est primordiale pour la qualité et la durabilité des échanges entre SOFIAP et ses clients.

L'accueil du client doit permettre d'obtenir toutes les informations utiles, notamment en matière d'identité et de capacité juridique, de revenus et de domicile.

S'agissant des clients personnes morales, SOFIAP vérifie que le représentant de la personne morale a la capacité d'agir, soit en sa qualité de représentant légal, soit au titre d'une délégation ou d'un mandat dont il bénéficie.

Cette phase de découverte initiale est aussi une opportunité pour comprendre les motivations du client à entrer en relation avec SOFIAP, sa situation, appréhender ses besoins et ses projets afin de proposer les solutions les plus appropriées.

Tous ces documents et informations doivent être collectés, saisis, classés et conservés dans le dossier client.

Basée sur la confiance, cette relation nécessite par ailleurs d'effectuer les diligences prévues en matière d'identification des risques susceptibles d'altérer cette relation, et d'adapter son niveau de vigilance en conséquence.

Dans ce cadre, les interrogations des fichiers d'incidents, en particulier ceux de La Banque de France, sont préalables à la finalisation de l'entrée en relation.

Concernant la lutte contre le blanchiment, la corruption et le financement du terrorisme, des diligences spécifiques doivent être exercées afin de disposer d'une connaissance approfondie de l'objet et de la nature des opérations envisagées, de l'origine des fonds, ainsi que du (des) bénéficiaire(s) effectif(s) de(s) l'opération(s) envisagée(s).

Ces exigences et vigilances sont maintenues tout au long de la relation commerciale, que les relations avec les clients soient en proximité ou distancées.

Ainsi, les entretiens doivent être préparés et anticipés afin d'optimiser les actions commerciales à engager. Ces rencontres avec le client sont l'occasion de mettre à jour l'ensemble des données constitutives de la connaissance client, et de s'assurer que les produits et services souscrits sont toujours adaptés à ses besoins et sa situation.

2.2.2. Informer les clients

SOFIAP veille à ce que ses clients disposent de l'ensemble des informations leur permettant de comprendre les caractéristiques des services et produits proposés, ainsi que les risques, les frais et les avantages et inconvénients y afférents. Ils doivent être en mesure de prendre leurs décisions en connaissance de cause.

Ces informations communiquées aux clients en temps utile doivent présenter un contenu clair, exact et non trompeur. En toute circonstance, SOFIAP veille à ce que les **communications** à destination des clients soient **loyales** et **transparentes**, et en particulier celles diffusées sur les **médias sociaux**.

Le domaine de l'assurance est concerné de la même manière par ces exigences, les clients devant disposer des fiches d'information et de conseil afin qu'ils puissent appréhender correctement les caractéristiques des produits, notamment celles liées aux garanties et exclusions, les tarifs...

Les clients sont mis en garde sur les risques éventuellement encourus quand ils souscrivent de leur propre initiative un produit qui n'apparaît pas adapté à leurs intérêts.

Les clients doivent disposer de l'ensemble des informations leur permettant de comprendre les caractéristiques des services et produits proposés par SOFIAP.

2.2.3. Documenter et tracer le conseil apporté aux clients

Le conseil nécessite de bien connaître les clients et de conserver tous les documents et informations utiles.

Il s'agit d'un préalable indispensable pour que SOFIAP soit en capacité de conseiller le client sur les produits et services les mieux adaptés à ses objectifs et à sa situation. En fonction des produits et services, un « test d'adéquation » est mené pour permettre de délivrer le conseil au client, et doit être formalisé et conservé de manière durable.

Dès lors que le client ne fournit pas les informations nécessaires, le conseiller s'abstient de fournir un conseil.

Une mise en garde du client doit être effectuée s'il apparaît une inadéquation du produit ou service proposé au client, ou si celui-ci ne fournit pas ou de manière insuffisante les informations nécessaires. La trace de cette mise en garde doit être conservée.

Dans le cas de produits dits complexes, ces obligations sont renforcées afin de s'assurer que le client comprend bien les caractéristiques, les risques, les avantages et les inconvénients du produit.

SOFIAP est habilitée à se fonder sur les informations fournies par le client, à moins qu'elle ne sache, que celles-ci sont manifestement périmées, erronées ou incomplètes. Dans ce dernier cas, SOFIAP agit au mieux des intérêts du client.

De manière générale, chaque collaborateur doit exécuter en temps voulu les instructions reçues de la clientèle, en tenant compte de leur nature et de leurs circonstances. Il doit conserver une preuve écrite de toute instruction.

2.3. Une démarche citoyenne de protection de la clientèle

2.3.1. Protection des données à caractère personnel

SOFIAP place la protection des données à caractère personnel au cœur de ses missions et des services proposés à ses clients.

L'ensemble des données à caractère personnel de ses clients, de ses collaborateurs, et de manière générale de toutes les personnes physiques dont elle est appelée à traiter les données dans le cadre de ses activités sont traitées dans le respect de la réglementation en matière de protection des données à caractère personnel.

En application du règlement général sur la protection des données (RGPD), SOFIAP veille à garantir l'information auprès des personnes concernées, la transparence, la sécurité et le respect des droits des personnes pour l'ensemble des traitements de données personnelles mis en œuvre.

SOFIAP s'engage à prendre toutes mesures afin d'assurer la sécurité et la confidentialité des données personnelles et notamment à empêcher qu'elles ne soient endommagées, effacées ou que des tiers non autorisés y aient accès.

Par ailleurs, en cas d'incident affectant les données personnelles traitées (destruction, perte, altération ou divulgation), SOFIAP s'engage à respecter l'obligation de notification des violations de données personnelles, notamment auprès de la CNIL mais aussi des personnes concernées le cas échéant.

Chaque personne concernée (clients, collaborateurs, autres, tiers, ...) par un traitement réalisé par SOFIAP, dispose à tout moment de la faculté d'exercer auprès de SOFIAP les droits prévus par la réglementation applicable en matière de données à caractère personnel, sous réserve d'en remplir les conditions :

- droit d'accès : elle peut avoir communication de ses données personnelles faisant l'objet d'un traitement par SOFIAP,
- droit de rectification : elle peut mettre à jour ses données personnelles ou faire rectifier ses données personnelles traitées par SOFIAP,
- droit d'opposition, notamment de faire l'objet d'actions de prospection commerciales par voie autre qu'électronique (SMS/email) de la part de SOFIAP : ladite personne peut exprimer son souhait de ne pas ou de ne plus recevoir de telles communications commerciales de la part SOFIAP ou de manière plus générale, demander que ses données personnelles ne fassent plus l'objet d'un traitement,
- droit à l'effacement : elle peut demander la suppression de ses données personnelles,
- droit à la limitation : elle peut demander la suspension du traitement de ses données personnelles,
- droit à la portabilité : elle peut demander à SOFIAP de récupérer ses données personnelles afin d'en disposer.

La désignation d'un délégué à la protection des données témoigne de l'attachement de SOFIAP à la protection des données personnelles de ses clients, de ses collaborateurs et autres partenaires.

Toute personne concernée peut contacter :

- le délégué à la protection des données à l'adresse suivante : La Banque Postale - Délégué à la Protection des Données - 115, rue de Sèvres - 75275 Paris Cedex 06 ; ou
- le référent à la protection des données de SOFIAP en adressant :
 - soit un courrier à SOFIAP – Cellule Protection des données - 64 rue de Saintonge 75003 Paris
 - soit un email à cellule_protectiondesdonnees@socrif.fr

2.3.2. Traitement des réclamations clients dans des délais appropriés

En cas de différend, le client a la possibilité de déposer une réclamation en ligne sur le site internet de SOFIAP ou la possibilité d'écrire reclamation@sofiap.fr ou SOFIAP, Service Réclamation, 64 rue de Saintonge, 75003 Paris.

SOFIAP s'engage à :

- accuser réception de la réclamation dans un délai maximum de 10 jours ouvrables, à compter de la date de son envoi par courrier ou de sa réception en ligne ou par email,
- apporter une réponse dans les plus brefs délais sans excéder le délai maximum de 60 jours ouvrables ;
- tenir le client informé en cas de dépassement de ce délai.

En cas de désaccord, le client peut exercer un recours, soit en ligne, soit en écrivant à reclamation@sofiap.fr ou à SOFIAP - Service Recours - Direction Juridique - 64 rue de Saintonge 75003 Paris.

Le service en charge du recours, procède à un nouvel examen du dossier et apporte une nouvelle réponse au client.

Le délai de réponse au recours est de 10 jours ouvrés maximum à compter de sa réception.

Si le différend persiste ou aucune réponse n'a été apportée à la réclamation dans un délai de deux mois, le client a la possibilité de saisir gratuitement le Médiateur de La Banque Postale qui facilitera la recherche d'une solution amiable :

- soit par courrier à l'adresse suivante : Le Médiateur de La Banque Postale – 115 rue de Sèvres – Case Postale G009 – 75275 PARIS CEDEX 06 ;
- soit en ligne sur le site Internet du Médiateur : <https://mediateur.grounelaposte.com>

2.3.3. Surveillance des situations de fragilité des clients

Des dispositifs de détection de situations potentielles d'états de faiblesse de clients, voire d'abus pouvant être commis à l'encontre des clients, sont mis en place au sein de SOFIAP.

Ces dispositifs visent à préserver la primauté des intérêts des clients tout en garantissant le respect du secret professionnel.

En cas de doute, les collaborateurs concernés par ces dispositifs engagent sans délai les diligences prévues et transmettent une signalisation aux interlocuteurs appropriés lorsque les situations le requièrent.

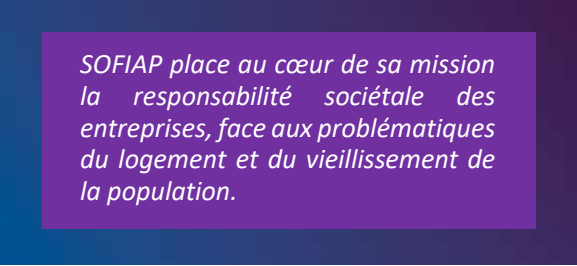
En cas de besoin, les mesures de sécurisation sont prises afin de préserver l'intérêt des différentes parties prenantes.

2.3.4. Recherche d'une relation responsable et durable avec les clients

SOFIAP s'engage à prévenir le surendettement, à accompagner les entreprises pour favoriser l'accession à la propriété de leurs salariés et aider ceux qui sont aidants afin de concilier plus sereinement leurs responsabilités professionnelles et leur rôle auprès de leur famille.

À ce titre, des accompagnements renforcés sont mis en place en cas de difficultés financières rencontrées par les clients fragiles.

Pour l'ensemble de ses clients, SOFIAP conçoit et propose une offre de produits et de services prenant en compte des critères de responsabilité sociétale des entreprises (RSE), notamment en matière d'éthique du conseil, de transparence, de simplicité et de clarté de l'offre.



SOFIAP place au cœur de sa mission la responsabilité sociétale des entreprises, face aux problématiques du logement et du vieillissement de la population.

2.3.5. Lutte contre la fraude

La fraude est un acte intentionnel ayant pour objectif d'obtenir un avantage matériel ou immatériel illégitime, au détriment d'une personne ou d'une organisation, perpétré notamment, en contrevenant aux lois, règlements ou règles et procédures internes.

La fraude interne fait intervenir la participation active ou passive d'un collaborateur soit isolément, soit en complicité avec des individus extérieurs (fraude mixte).

Elle se définit comme « **un détournement de fonds ou de biens (y compris de données) commis intentionnellement selon un procédé illicite, par un collaborateur dans l'exercice de ses fonctions afin d'en tirer un avantage souvent financier** ».

Exemples de typologies de fraudes internes : malversations par détournement de fonds - abus de faiblesse - falsification/contrefaçon de documents - vol/compromission de données clients - vol d'informations internes/stratégiques - détournement d'outils professionnels - contrefaçon/ détournement de moyens de paiement - manipulations de comptes/caisses ...

La fraude interne **inclut également les comportements déloyaux de collaborateurs permettant la commission de la fraude**. Cela se traduit par le **non-respect intentionnel des fonctions exercées, des délégations accordées et des règles définies par l'entité** dans chaque domaine d'activité.

SOFIAP s'engage pour une politique de **tolérance zéro en matière de fraude interne**. Tout collaborateur contrevenant aux règles de bonne conduite s'expose à des sanctions disciplinaires. Par ailleurs, SOFIAP pourra déposer une plainte pénale à l'encontre de tout collaborateur auteur d'une fraude interne.

La lutte contre la fraude est l'affaire de tous. Chaque collaborateur doit apporter son concours à la prévention de la fraude et assurer une vigilance constante dans le cadre de son activité.

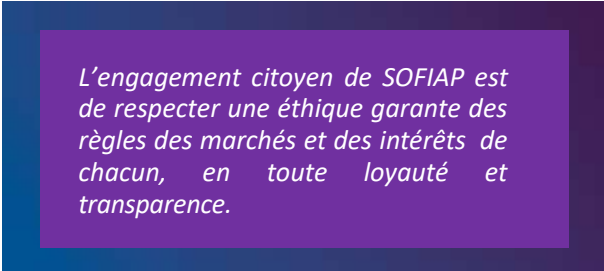
Tous les collaborateurs de SOFIAP sont invités à alerter sur des faits pouvant constituer une fraude notamment à travers le dispositif d'alerte.

3. Règles de bonne conduite vis-à-vis des marchés et des parties prenantes

Dans le cadre de ses activités, SOFIAP est en relation constante avec les différents acteurs des marchés bancaires, financiers et d'assurance, tels les organismes de tutelle, de supervision et de réglementation, les établissements financiers concurrents, les organismes professionnels...

Par ailleurs, SOFIAP entretient quotidiennement des relations d'affaires avec des prestataires, des tiers et partenaires qui l'accompagnent dans son développement.

Vis-à-vis de toutes ces parties prenantes, l'engagement citoyen de SOFIAP est de respecter une éthique garante des règles des marchés et des intérêts de chacun, en toute loyauté et transparence.



L'engagement citoyen de SOFIAP est de respecter une éthique garante des règles des marchés et des intérêts de chacun, en toute loyauté et transparence.

Tous les collaborateurs de SOFIAP concourent à l'atteinte de cette exigence.

3.1. Respect des règles en matière de concurrence

SOFIAP, fidèle à son image citoyenne, ainsi que ses dirigeants, se sont engagés à respecter et à faire respecter au sein de SOFIAP un développement commercial dans le strict respect du droit de la concurrence.

SOFIAP proscrit tout manquement au droit de la concurrence et attend de ses collaborateurs qu'ils s'inscrivent dans une démarche de tolérance zéro. Sont proscrits tous les comportements qui pourraient être considérés comme constitutifs d'une pratique anticoncurrentielle en toute circonstance, et plus particulièrement à l'occasion de négociations commerciales, au sein de filiales communes du Groupe La Banque Postale, dans les groupes de travail interbancaires de Place, au sein des organisations professionnelles telles que L'Association française des Sociétés Financières (ASF).

Ces comportements peuvent notamment consister :

- en tout type d'accord, toute entente même non écrite avec des concurrents ou partenaires visant en fait ou en droit à limiter la concurrence sur un marché,
- à tout échange d'informations commerciales sensibles relatives à la stratégie commerciale de SOFIAP, à sa politique de prix, ses marges, à ses clients, aux campagnes de communication à venir,
- ou plus globalement tout échange susceptible d'exercer une influence sur la politique commerciale de l'entreprise.

À cette fin SOFIAP met en œuvre un programme de conformité concurrence dont l'objectif est de former/sensibiliser ses collaborateurs au mérite d'avoir en toutes circonstances un comportement professionnel qui soit conforme aux principes et aux règles du droit de la concurrence.

Chaque collaborateur est garant de ces règles. Pour en assurer le strict respect et éviter toute action judiciaire qui serait née de pratiques anticoncurrentielles, SOFIAP a mis en place un dispositif sécurisé et confidentiel qui permet à chacun de signaler un comportement susceptible de constituer une violation du droit de la concurrence ou de faire part de ses doutes quant à la compatibilité d'une situation constatée avec les principes émis ci-dessus. **Ce dispositif s'inscrit dans le cadre du droit d'alerte général prévu au § 1.1.8 du code de conduite.**

3.2. Respect des engagements citoyens

3.2.1. Responsabilité sociétale de SOFIAP

Fort de son ADN citoyen, SOFIAP vise à cultiver une relation de confiance avec ses clients, fondée sur la qualité du conseil, l'écoute et la transparence.

Cette ambition se traduit par une offre produits inclusive prenant en compte les critères ESG (environnementaux, sociaux, gouvernance). À ce titre, SOFIAP s'est fixée l'objectif d'être le 1^{er} partenaire des entreprises qui au travers du prêt subventionné peuvent efficacement favoriser l'accession à la propriété de leurs salariés et aider ceux qui sont aidants afin de concilier plus sereinement leurs responsabilités professionnelles et leur rôle auprès de leur famille.

Les règles de déontologie et les réflexions conduites dans ce domaine, ainsi que la prise en charge des situations de fragilité financière des clients, sont parties prenantes de cet engagement sociétal qui concerne l'ensemble des collaborateurs de SOFIAP.

3.2.2. Politique d'achats responsables

La politique achats responsables de La Poste Groupe sert de document de référence dans la démarche achats responsables de SOFIAP. Elle s'inscrit dans une démarche responsable, éthique et transparente et permet d'établir des relations de confiance avec les fournisseurs et sous-traitants.

Cette approche se traduit concrètement par la réaffirmation, dans la politique achats responsables de SOFIAP du pilier 1 : « faire respecter les droits fondamentaux et les promouvoir tout au long des chaînes d'approvisionnement ». Ces principes sont rappelés et complétés dans le corpus documentaire et contractuel de SOFIAP auprès de chaque partie prenante (fournisseurs et sous-traitants, prescripteurs et acheteurs) notamment :

- au travers de la **charte achats responsables et éthique du Groupe La Banque Postale**, annexée systématiquement dans les contrats de prestations, produits et services signés entre SOFIAP et ses fournisseurs et sous-traitants,
- les conditions générales d'achats figurant au verso de tout bon de commande émis par SOFIAP intègrent la « lutte contre la corruption et devoir de vigilance », l'engagement du fournisseur, à travers l'exécution de ce bon de commande, à respecter l'ensemble des lois, réglementations et normes internationales, notamment en termes de respect des droits humains et libertés fondamentales.

Cette approche également énoncée dans les piliers 3 : « favoriser l'inclusion sociale et contribuer au développement du tissu économique et social des territoires à travers nos achats » et 4 : « consolider les relations responsables et éthiques avec nos fournisseurs » de la politique achats responsables se traduit par l'intégration de critères extra-financiers dans la sélection et le suivi des fournisseurs, le recours au secteur protégé/adapté, et l'accessibilité des petites et moyennes entreprises aux appels d'offres de SOFIAP.

Cette orientation forte se traduit aussi dans le processus achats par la prise en compte de principes déontologiques visant à garantir l'indépendance de jugement des acheteurs et décideurs, la transparence vis-à-vis des fournisseurs et sous-traitants, la traçabilité des actes d'achat, et la volonté de lutter contre toute forme de corruption.

Dans ce cadre, les prescripteurs, acheteurs, décideurs s'engagent à signaler au plus tôt tout conflit d'intérêts qui serait susceptible d'interférer dans le processus achats.

Ce processus achats précise aussi le rôle des collaborateurs et l'importance d'une mise en concurrence saine et loyale à l'occasion des appels d'offres.

Les données à caractère personnel transmises dans le cadre d'un marché font l'objet d'une sécurisation renforcée notamment via des clauses dédiées et intégrées dans le processus achats.

4. Règles de conduite applicables à la lutte contre la corruption et au trafic d'influence

L'ensemble des règles et des comportements attendus, définis dans le code de conduite anti-corruption de SOFIAP annexé à son règlement intérieur sont applicables aux collaborateurs et dirigeants de SOFIAP.

4.1. Engagement de SOFIAP

SOFIAP s'engage pour une politique de tolérance zéro en matière de corruption.

Cet engagement se traduit par 3 grands principes en matière de prévention de la corruption qui s'appliquent à l'ensemble des collaborateurs, quel que soit leurs fonctions ou leur lieu de travail :

- 1^{er} principe : tolérance zéro,
- 2^e principe : tous concernés,
- 3^e principe : tous vigilants.

L'engagement de SOFIAP et de ses dirigeants s'appuie sur un programme de détection et de prévention de la corruption, conformément aux dispositions de la loi Sapin 2⁵⁸.

Ce programme permet de prévenir la survenance de faits de corruption mais aussi d'identifier les pratiques et les situations à risques.

Le programme se décline en huit mesures :

1. un code de conduite qui définit les comportements à proscrire,
2. un dispositif d'alerte interne qui permet aux collaborateurs de signaler de possibles comportements ou situations contraires au code de conduite,
3. une cartographie des risques de corruption régulièrement actualisée,
4. des procédures d'évaluation de l'intégrité des tiers (clients, fournisseurs, partenaires commerciaux et non-commerciaux, cibles de prise de participation ou de fusion/acquisition),
5. des procédures de contrôles comptables spécifiques, dédiées à la détection de la corruption,
6. un dispositif de formation à destination de l'ensemble des collaborateurs de l'entreprise y compris les personnels les plus exposés au risque de corruption,
7. un régime disciplinaire encadrant les faits d'atteinte à la probité au sein de l'entreprise,
8. un dispositif de contrôle et d'évaluation interne de l'ensemble de ces mesures.

La mise en œuvre de ce programme repose sur :

- une fonction Conformité Groupe, dirigée par le Directeur de la Conformité Groupe,
- une Direction dédiée à la déontologie, à la lutte contre la corruption et au devoir de vigilance, rattachée hiérarchiquement au Directeur de la Conformité Groupe,
- un réseau de correspondants chargés de la mise en œuvre du programme, dont la Directeur de la Conformité de SOFIAP ;
- un reporting régulier à destination du Directoire et du Comité d'Audit et des Risques du Conseil de Surveillance de SOFIAP.

4.2. Définitions

La corruption

La corruption est prévue et punie par le code pénal. Elle peut être active ou passive.

La corruption active est le fait, pour une personne physique ou morale (le corrupteur), de proposer des offres, promesses,

⁵ 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

dons, présents ou des avantages quelconques à une personne publique ou une personne privée exerçant dans un cadre professionnel (le corrompu) pour qu'elle accomplisse ou s'abstienne d'accomplir, un acte de sa fonction, de sa mission ou de son mandat, ou facilité par sa fonction, sa mission ou son mandat.

C'est aussi le fait pour le corrupteur de céder à des sollicitations de la part du corrompu.

La corruption passive est le fait pour une personne publique ou privée exerçant dans un cadre professionnel d'accepter d'être corrompue ou de solliciter un corrupteur aux fins d'être corrompue.

La corruption naît dès que la personne tente d'obtenir un avantage d'une autre personne, même si celle-ci finalement n'entre pas dans la relation de corruption.

Toute personne qui aura incité à la corruption, ou qui aura aidé ou facilité en connaissance de cause son exécution pourra être reconnue coupable de complicité de corruption, également illégale.

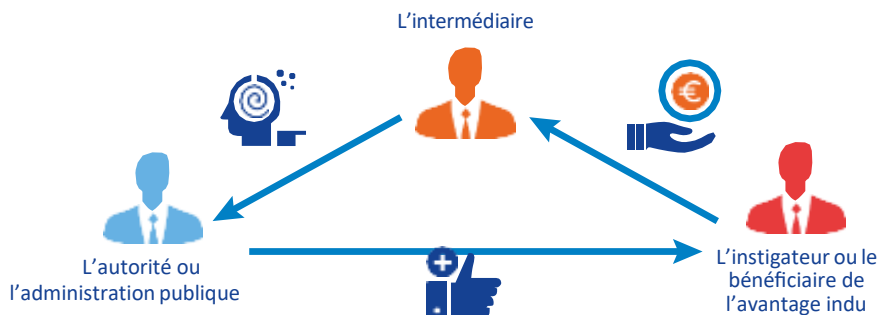


Le trafic d'influence

SOFIAP s'est engagée à prévenir les risques relatifs au trafic d'influence commis par une personne dépositaire de l'autorité publique, chargée d'une mission de service public, ou investie d'un mandat électif.

Est considéré comme trafic d'influence le fait pour une personne physique ou morale de proposer des offres, promesses, dons, présents ou des avantages quelconques à une personne publique ou une personne privée exerçant dans un cadre professionnel, pour abuser de son influence réelle ou supposée en vue de faire obtenir d'une autorité publique ou d'une administration, des distinctions, des emplois, des marchés ou toute autre décision favorable.

La loi distingue également, comme pour la corruption, le trafic d'influence actif et le trafic d'influence passif.



Les sanctions en matière de corruption :

• Sanctions pour les collaborateurs :

Sanctions pénales pour corruption d'agent public français ou étranger :

- 10 ans de prison,
- 1 000 000 euros d'amende ou le double du produit tiré de l'infraction.

Sanctions pénales pour corruption privée :

- 5 ans de prison,
- 500 000 euros d'amende ou le double du produit tiré de l'infraction.

Peines complémentaires :

- privation des droits civiques,
- interdiction d'exercer l'activité litigieuse pendant 5 ans ou plus,
- inéligibilité (jusqu'à 10 ans),
- sanction disciplinaire, y compris radiation des cadres ou licenciement.



Corruption publique : corruption impliquant un agent exerçant une fonction publique (fonctionnaire, salarié, chargé d'une mission de service public ...)

Corruption privée : corruption impliquant un agent n'exerçant pas de fonction publique et agissant dans le cadre d'une activité professionnelle

• Sanctions pour l'entreprise :

Sanctions pénales pour corruption publique :

- 5 000 000 euros d'amende,
- ou 10 fois le produit tiré de l'infraction

Sanctions pénales pour corruption privée :

- 2 500 000 euros d'amende,
- ou 10 fois le produit tiré de l'infraction

Sanctions complémentaires :

- exclusion des marchés publics pendant 5 ans sur tout le territoire de l'UE,
- fermeture de l'établissement (ou des établissements),
- interdiction de lever des fonds,
- interdiction de monter des projets avec des organisations comme La Banque Mondiale par exemple.

De lourds préjudices en jeu :

- financier,
- atteinte à la réputation,
- responsabilité pénale des dirigeants.

Ces mêmes sanctions s'appliquent en matière de trafic d'influence.

4.3. Illustrations

1^{re} illustration

Vous recevez un client pour monter un dossier de prêt. Ce client n'est pas éligible aux conditions du financement. Comme il travaille dans le secteur du tourisme, il vous propose des conditions très avantageuses sur un séjour à l'étranger dont vous lui avez parlé, en contrepartie de votre aide pour obtenir son financement.

Le client cherche à influencer votre décision en contrepartie d'un avantage. En acceptant cette offre vous commettez un acte de corruption.

2^e illustration

Vous êtes collaborateur et par ailleurs élu local. Un client vous demande d'interférer auprès du décideur public pour obtenir un permis de construire, en échange d'un petit plus en espèces.

Le client cherche à utiliser votre influence. En acceptant cette proposition, vous participez à un trafic d'influence.

3^e illustration

Vous connaissez le responsable d'une entreprise spécialisée dans l'un des secteurs pour lesquels vous allez lancer un appel d'offres. Il vous invite à dîner et vous demande de faire une faveur à sa société en la retenant dans le panel.

Vous devez refuser l'invitation dans la mesure où vous êtes en période d'appel d'offres. Si vous acceptez cela pourrait être considéré comme un acte de corruption.

4^e illustration

Vous êtes invité par un de vos prestataires à participer à un séminaire. Ce prestataire se propose de vous payer tous vos frais et il prévoit votre séjour dans un hôtel prestigieux.

Vous devez refuser et en parler avec votre responsable hiérarchique afin d'éviter tout soupçon de corruption dans votre relation avec le prestataire.

5^e illustration

Un partenaire ou prestataire vous demande de ne pas mettre à jour les diligences réglementaires en échange d'un séjour dans un bel établissement en France. Ce dernier cherchait à dissimuler une condamnation récente.

En acceptant cette offre vous commettez un acte de corruption.

6^e illustration

Une association souhaite bénéficier d'un contrat de sponsoring. Cette association approche un collaborateur et lui propose de bénéficier de places pour les prochains Jeux Olympiques en échange de ce contrat de sponsoring.

Les opérations de sponsoring ou de mécénats sont légales mais ne peuvent toutefois pas être réalisées dans l'intention d'obtenir un avantage indu ou de dissimuler une contrepartie. En acceptant cette offre vous commettez un acte de corruption.

4.4. Situations à risques et comportements attendus de la part des collaborateurs

Tout collaborateur doit exercer une vigilance particulière dans les situations suivantes :

- les relations avec les tiers, (partenaires, prestataires, sous-traitants) et en particulier les intermédiaires (consultants, agents commerciaux, apporteurs d'affaires) en vérifiant notamment leur intégrité, et pour ce faire, en interrogeant la Direction de la Conformité,
- les interactions avec les agents publics et le secteur public local,
- le mécénat et le sponsoring,
- les paiements de facilitation,
- le financement de partis politiques, syndicats,
- les situations de conflits d'intérêts,
- les cadeaux et invitations.

Les relations avec les tiers :

On entend par « tiers » les parties prenantes avec lesquelles SOFIAP est en relation ou envisage d'entrer en relation d'affaires, les parties prenantes avec lesquelles SOFIAP est en relation d'affaires (clients personnes physiques ou personnes morales, fournisseurs, partenaires commerciaux ou non commerciaux, intermédiaires, apporteurs d'affaires...etc.).

La vigilance de tous est appelée sur la rigueur qui doit être apportée dans la démarche d'évaluation de l'intégrité de ces tiers, tout au long de la relation et notamment au moment de l'entrée en relation afin d'éviter que SOFIAP se trouve impliquée directement ou indirectement dans des tentatives de corruption voire dans des affaires de corruption.

Les collaborateurs doivent respecter les procédures mises en œuvre par SOFIAP afin de s'assurer que les tiers présentent des garanties suffisantes en termes d'intégrité :

- [20.02 - Procédure Evaluation des Tiers](#),
- [20.03 - Procédure revue des risques de corruption PPE](#).

Ces dispositions visent à prémunir SOFIAP de toute atteinte à son image et à sa réputation.

Elles varient en fonction des catégories de tiers (clients personnes physiques ou morales, fournisseurs et prestataires, partenaires commerciaux et non commerciaux, cibles de fusion/acquisition). Elles visent toutes à apprécier le risque de manquement à la probité⁶ spécifique induit par la relation entretenue ou qu'il est envisagé d'entretenir avec un tiers donné.

Dès lors qu'un doute survient sur l'intégrité d'un tiers avec lequel SOFIAP est en relation d'affaires ou envisage de l'être, les collaborateurs doivent se rapprocher de la Direction conformité métier ou de la direction déontologie – anticorruption.

Les indices suivants sont susceptibles de constituer des signaux d'alarme :

- la partie prenante semble manquer de personnel, ne bénéficier d'aucune expérience, y compris sur le marché, être une coquille vide ou avoir une structure opaque, refuser de divulguer l'identité de ses propriétaires réels ou d'autres propriétaires indirects,
- la partie prenante recommande l'intervention d'un intermédiaire,
- la partie prenante demande à rester anonyme,
- le paiement des honoraires de l'intermédiaire est inhabituel ou excessif au regard de sa mission, ou sans justificatifs suffisants par rapport aux prestations,
- le pays ou le secteur dans lequel a lieu la prestation est connu pour avoir un fort taux de corruption⁷,
- l'intermédiaire suggère qu'une certaine somme d'argent est nécessaire au préalable afin de s'assurer un contrat public ou de conclure une affaire,
- l'accord avec l'intermédiaire est non-écrit, ou écrit sans définir de commission spécifique ou de calendrier de paiement,
- le calendrier de paiement défini dans le contrat de l'intermédiaire est clairement excessif au regard de la quantité de travail qui sera entreprise,
- l'intermédiaire exige des modalités de paiement inhabituelles, comme un paiement en nature ou en liquide, ou encore un paiement redirigé vers un compte ouvert dans un autre pays.

⁶ Les faits de corruption, de trafic d'influence, de concussion, de prise illégale d'intérêt, de détournement de fonds publics, de favoritisme

⁷ Indice de perception de la corruption de Transparency International

Interactions avec des agents publics

Les relations d'affaires impliquant des personnes politiquement exposées (PPE), des agents publics ou des intermédiaires, doivent faire l'objet d'une vigilance accrue.

Mécénat et sponsoring :

Le risque est que les sommes payées masquent le versement de pots-de-vin si l'objet du mécénat ou du sponsoring a une relation directe ou indirecte avec un tiers (ou l'un de ses proches) dont il est attendu une contrepartie.

Les contrats de sponsoring, au même titre que les autres partenariats doivent respecter les processus internes et faire l'objet d'une évaluation de l'intégrité du tiers. Il est rappelé que :

- les dons/participations ne doivent pas être en liquide, ni versés sur le compte d'une personne physique,
- les dons/participations ne doivent pas être liés à l'exécution d'une transaction commerciale,
- les paiements par le truchement de tiers sont à proscrire.

Paievements de facilitation :

Les « paiements de facilitation » sont des paiements effectués afin d'inciter un agent public étranger à exécuter des tâches relevant de sa fonction. Les paiements sont généralement d'un montant très limité et conçus pour accélérer des actions de routine d'agents publics qui sont susceptibles d'intervenir dans la « transaction » (obtention de visas, permis, documents administratifs).

Toute tentative pour obtenir ou offrir des paiements de facilitation doivent être immédiatement rapportés au déontologue.

Financement de partis politiques :

Le financement de partis politiques est strictement interdit.

Conflits d'intérêts :

Pour prévenir ce risque, SOFIAP s'est dotée d'une Politique de prévention et de gestion des conflits d'intérêts qui vise à :

- appréhender la notion de conflits d'intérêts et ses enjeux pour SOFIAP,
- renforcer les mesures d'identification, de prévention et de gestion des conflits d'intérêts.

Les règles afférentes à la prévention et à la gestion des conflits d'intérêts sont prévues au paragraphe dédié à cet effet.

Cadeaux et invitations :

L'ensemble des règles encadrant les cadeaux et invitations sont décrites au § 1.3 Politique cadeaux et invitations.

4.5. Prévention des actes de corruption

La prévention des actes de corruption passe par des actions de formation des collaborateurs de SOFIAP et la mise à disposition du dispositif d'alerte ouvert aux collaborateurs et aux tiers.

Formation :

Le programme de formation et de sensibilisation est essentiel : il permet la diffusion et l'appropriation par tous les collaborateurs de la Politique anticorruption et des engagements pris par le Directoire. Ces actions permettent de constituer une culture et un socle de connaissances commun.

Les collaborateurs de SOFIAP sont soumis à l'obligation de réaliser les formations dispensées en matière de prévention de la corruption en particulier les cadres et les personnels les plus exposés au risque de corruption.

Le dispositif de formation permet de sensibiliser les collaborateurs et d'acquérir les bons réflexes face à la survenance éventuelle d'une situation de corruption.

Dispositif d'alerte :

Tous les collaborateurs de SOFIAP sont invités à alerter sur des faits pouvant constituer un comportement contrevenant aux principes du code de conduite, notamment en cas de corruption.

L'émetteur de l'alerte doit présenter de manière objective des faits concernant l'un des cas suivants :

- un manquement aux règles du code de conduite,
- un crime ou un délit,
- une violation d'un engagement international, d'un acte unilatéral d'une organisation internationale, de la loi ou du règlement,
- une menace ou un préjudice grave pour l'intérêt général.

Le dispositif d'alerte est accessible à l'adresse suivante : www.alerte-ethique.laposte.fr.

SOFIAP met en œuvre les diligences appropriées pour assurer la confidentialité des faits signalés et de l'émetteur de l'alerte.

Une procédure spécifique détaille les modalités de traitement des signalements. Cette procédure est accessible à tous les collaborateurs sur l'Intranet de SOFIAP.

Contrôle du dispositif :

SOFIAP met en place un dispositif de contrôle adapté et proportionné aux risques auxquels elle est exposée. Ces contrôles sont organisés à trois niveaux :

- contrôle permanent de 1er niveau,
- contrôle permanent de 2e niveau,
- contrôle périodique de 3e niveau.

Les résultats de ces contrôles alimentent notamment la cartographie des risques de corruption.

4.6. Sanctions

Le non-respect par un collaborateur des règles établies au titre de la lutte contre la corruption (code de conduite, politique et procédures), engage la responsabilité personnelle de celui-ci et pourra l'exposer à des sanctions disciplinaires conformément aux dispositions applicables dans l'entreprise, pouvant aller jusqu'au licenciement, selon la gravité du manquement.

En outre, la violation de ces règles est susceptible d'exposer le collaborateur à des poursuites judiciaires, civiles et/ou pénales.

5. Lutte contre le blanchiment et le financement du terrorisme

Afin de lutter contre le blanchiment de capitaux⁸ et le financement du terrorisme⁹ et garantir le respect des sanctions nationales et internationales¹⁰, SOFIAP s'engage à respecter toutes les lois et réglementations en vigueur et à promouvoir des règles claires en la matière.

À ce titre, SOFIAP s'est dotée d'un dispositif de maîtrise des risques de blanchiment de capitaux et de financement du terrorisme reposant notamment sur la mise en place d'une classification et d'une cartographie des risques LCB-FT, d'un corpus normatif de sécurité financière complet et de contrôles adaptés.

SOFIAP s'assure qu'une culture conformité est en permanence diffusée en son sein. À cet égard, SOFIAP organise des cycles de formations obligatoires, spécifiques et adaptées, dispensées aux collaborateurs. Ces derniers – quelles que soient les équipes et les lignes métiers - ont le devoir de les suivre afin de garantir un niveau de vigilance adéquat dans le cadre de l'exercice de leurs missions et de lutter efficacement contre le blanchiment de capitaux et le financement du terrorisme.

Le dispositif LCB-FT s'appuie en outre sur une connaissance client complète et actualisée, la mise en œuvre d'une vigilance constante, un dispositif de détection des opérations atypiques et le strict respect des mesures de gels des avoirs et des sanctions internationales qui repose sur les collaborateurs et des outils spécifiques.

5.1. Connaissance clients (KYC)

Dans le cadre de leur mission et pour s'assurer d'agir dans l'intérêt exclusif des clients, les collaborateurs de SOFIAP doivent effectuer toutes les diligences nécessaires pour connaître les clients y compris leurs activités et leurs produits en :

- collectant et vérifiant les informations d'identification des clients,
- se renseignant sur la nature et l'objet de la relation d'affaires,
- s'assurant que les informations recueillies sont en cohérence avec le profil du client,
- renseignant correctement les informations collectées dans les différents systèmes d'information,
- maintenant une connaissance actualisée de la relation d'affaires par la mise en place d'une revue périodique et événementielle et à l'occasion de chaque rencontre clients,
- conservant les documents collectés selon les règles édictées par les procédures de SOFIAP.

5.2. Vigilance constante des opérations

SOFIAP a mis en place des mesures permettant de s'assurer de la cohérence des opérations effectuées en s'appuyant sur une connaissance actualisée de la relation d'affaires ainsi que la détection et l'analyse des opérations inhabituelles.

Cette détection d'opération inhabituelle repose sur un système automatisé et sur une vigilance humaine.

À ce titre, les collaborateurs de SOFIAP doivent être vigilants afin de détecter et prévenir les opérations qui seraient inhabituelles. Ces opérations doivent être signalées à la Direction de la Conformité afin qu'une analyse plus poussée puisse être effectuée.

À la suite de l'analyse, une déclaration de soupçon doit être transmise à Tracfin, s'il existe des soupçons que les sommes ou opérations :

- proviennent d'une infraction passible d'une peine privative de liberté supérieure à un an,
- participent au financement du terrorisme,
- sont le produit d'une fraude fiscale selon les critères prévus par la réglementation.

⁸ Le blanchiment de capitaux est le fait de masquer l'origine illégale des revenus issus d'activité délictueuse.

⁹ Le financement du terrorisme est le fait de fournir ou de réunir des fonds, d'origine légale ou illégale, susceptibles d'être utilisés pour commettre un acte terroriste.

¹⁰ Les sanctions internationales sont des mesures prises par un ou plusieurs États à l'encontre de personnes physiques et/ou morales (par exemple le gel des avoirs), mais également à l'encontre de pays ou de gouvernements (mesures d'embargo). Elles ont notamment pour objectif de lutter contre le terrorisme, les activités de prolifération nucléaire et les violations des droits de l'homme.

Toute décision de procéder à une déclaration de soupçons ou à un classement sans suite doit être dûment motivée, justifiée et faire l'objet d'une piste d'audit.

5.3. Lutte contre le financement du terrorisme et respect des embargos

Afin de prévenir le financement du terrorisme, SOFIAP veille à l'application des mesures de gel des avoirs financiers susceptibles de profiter à des personnes ou entités en lien avec des activités terroristes ou soumises à des sanctions internationales.

Cela se traduit par le fait de mettre en place un système de criblage des bases clients afin de détecter des personnes visées par des mesures de gel des avoirs ou des opérations interdites par des sanctions internationales.

En cas d'alerte avérée, il conviendra de :

- pour un prospect, refuser l'entrée en relation,
- pour un client, de soumettre toute opération à la validation de la Direction de la Conformité,
- pour une opération en contradiction avec les sanctions internationales, ne pas réaliser l'opération et le cas échéant geler les fonds,
- être vigilants pour détecter et prévenir tout contournement de mesures de gel des avoirs ou de sanctions financières.

5.4. Coopération avec les autorités de surveillance et de régulation

SOFIAP et ses collaborateurs doivent coopérer avec les autorités de surveillance ou de régulation, en fournissant des informations exactes et transparentes.

6. Politique fiscale

L'obligation de se conformer à toutes les réglementations fiscales françaises ou étrangères en vigueur et applicables aux opérations gérées pour le compte de ses clients et pour son propre compte est un engagement prioritaire pour le Groupe La Banque Postale.

La politique fiscale vise à harmoniser les pratiques fiscales au sein du Groupe, tout en préservant les spécificités locales et en respectant les règles de conformité du Groupe. Elle couvre tous les impôts et taxes prévus par les réglementations fiscales françaises ou étrangères applicables aux opérations réalisées par ses clients et pour son propre compte.

Dans ce contexte de conformités réglementaires, deux objectifs directeurs sont poursuivis par SOFIAP.

6.1. Recherche d'une maîtrise de la charge fiscale

SOFIAP a pleinement conscience de l'importance des impôts et taxes comme sources de recettes publiques ainsi que de leur contribution à la stabilité macroéconomique et au développement durable d'un pays. Elle a à cœur d'être exemplaire en matière de bonnes pratiques fiscales et ainsi être en cohérence avec sa raison d'être : œuvrer pour une transition juste en créant de la valeur durable et partagée, en soutenant la vitalité des territoires tout en respectant les limites environnementales de la planète.

Dans les relations avec ses clients, SOFIAP s'interdit de promouvoir et de participer à la réalisation d'opérations ayant pour seul motif d'éviter ou de permettre l'obtention d'un avantage fiscal indu. Elle s'engage également à ne pas soutenir des opérations permettant de faciliter ou soutenir des opérations avec ses clients dont l'efficacité repose sur la non-transmission d'informations aux autorités fiscales ou ont pour but de participer à contrevenir aux lois ou réglementations fiscales. Pour l'ensemble de ses projets, pour compte propre ou pour ses clients, SOFIAP s'assure que l'objectif de la transaction, qu'il soit économique ou patrimonial, doit être non artificiel, cohérent, crédible et conforme aux intentions du législateur. **Les opérations à but essentiellement fiscal sont en conséquence interdites.**

Dans ses relations auprès des autorités fiscales, SOFIAP veille à maintenir une relation professionnelle de qualité et de confiance en s'attachant aux respects des droits et devoirs de la Banque dans le respect des textes.

SOFIAP s'interdit toute implantation dans un état figurant dans la liste officielle française des états et territoires non coopératifs (ETNC) ou liste européenne des paradis fiscaux en vigueur. Elle veille à respecter les règles fiscales prévues par les lois, règlements et traités internationaux.

La politique de prix de transfert s'applique selon les normes du Groupe La Poste.

6.2. Maîtrise du risque fiscal

SOFIAP s'applique à maîtriser le risque fiscal, tel un défaut ou retard dans la déclaration ou le paiement des impôts, un défaut ou erreur d'interprétation dans l'application de la réglementation.

DÉONTOLOGIE

Votre code de conduite

Annexes

Les engagements et règles de déontologie présentés dans ce code de conduite s'appliquent à tout collaborateur exerçant ses activités au sein de SOFIAP et toute personne agissant, ou réalisant des opérations au nom et pour le compte de SOFIAP.

Table des matières

1. Annexe 1 : Charte utilisateur des moyens informatiques	57
1.1. Préambule	57
1.2. Droits et devoirs des utilisateurs	58
1.2.1. Dispositions générales	58
1.2.2. Dispositions relatives à l'usage à titre personnel des ressources informatiques	58
1.2.3. Dispositions relatives à la protection des équipements	59
1.2.4. Dispositions relatives à la protection des informations	59
1.2.5. Dispositions spécifiques à l'accès aux systèmes d'information	60
1.2.6. Dispositions spécifiques à l'utilisation de la messagerie électronique	61
1.2.7. Dispositions spécifiques à l'utilisation de l'internet	61
1.2.8. Dispositions relatives à l'utilisation de la téléphonie	62
1.2.9. Dispositions relatives aux équipements mobiles	62
1.2.10. Comportement en cas d'incident	63
1.2.10.1. Devoir général d'alerte	63
1.2.10.2. Attaque par code malveillant ou intrusion sur le poste de travail	63
1.2.10.3. Vol ou perte d'une ressource	63
1.3. Contrôles et collecte d'informations	64
1.4. Sanctions	64
2. Annexe 2 : Charte administrateur des moyens informatiques	65
2.1. Préambule	65
2.2. Administrateurs informatiques	65
2.2.1. Les pouvoirs de l'administrateur informatique	65
2.2.2. Les devoirs de l'administrateur informatique	66
2.2.2.1. Confidentialité	66
2.2.2.2. Protection et utilisation appropriée des droits d'accès	66
1.1.1.1. Respect de la « politique de sécurité des systèmes d'information du groupe La Banque Postale »	67
1.1.1.2. Devoir d'alerte	67
1.1.1.3. Sensibilisation à la sécurité informatique	67
1.2. Traçabilité et contrôle	68
1.3. Sanctions	68

Annexe 1 : Charte utilisateur des moyens informatiques

1.1. Préambule

Les systèmes d'information constituent pour SOFIAP une ressource stratégique indispensable à la conduite de ses activités et à la satisfaction de ses clients.

Ces systèmes d'information sont exposés à de nombreux risques en termes de sécurité (notamment virus, vers, messages indésirables, piratages et fraudes informatiques), et encadrés par des exigences légales, réglementaires et contractuelles de plus en plus strictes.

Dans ce contexte, une politique de sécurité des systèmes d'information, dont la présente charte est un des principaux éléments, a été définie par SOFIAP. Elle fixe les règles et précautions que doit respecter tout utilisateur des systèmes d'information, afin d'adopter un comportement professionnel, soucieux de la sécurité des systèmes d'information, à même de garantir un usage fiable et sécurisé des systèmes d'information de SOFIAP.

« L'utilisateur » joue un rôle essentiel dans ce dispositif.

La sécurité des systèmes d'information est l'affaire de chacun.

La présente charte relative à l'utilisation des ressources des systèmes d'information de SOFIAP précise les **responsabilités de tout utilisateur** de ces systèmes d'information.

À ce titre, la charte vise trois objectifs principaux :

- **sensibiliser** les utilisateurs à la protection du patrimoine informationnel de SOFIAP, et aux principes de sécurité des systèmes d'information qu'elle implique,
- **informer** tout utilisateur de ses droits et devoirs en matière d'utilisation des ressources informatiques mises à sa disposition pour la réalisation de sa mission dans l'entreprise,
- porter à la **connaissance** de chaque utilisateur les moyens utilisés par SOFIAP pour assurer le **contrôle** de l'utilisation des ressources des systèmes d'information.

Les principes développés dans le présent document s'appliquent à tous les collaborateurs de SOFIAP, CDI, CDD, stagiaire, alternant, ainsi qu'à toute personne agissant « au nom et pour le compte » de SOFIAP et également aux intérimaires, consultants et autres prestataires de services.

La charte s'applique à toutes les ressources des systèmes d'information mises à la disposition des utilisateurs par SOFIAP. Le terme de « ressource » englobe « contenant » et « contenu », à savoir :

- l'information elle-même, indépendamment de sa nature et de son support de stockage (papier, numérique) et notamment toute donnée saisie, collectée, traitée ou stockée, que SOFIAP utilise dans le cadre de ses activités,
- les systèmes informatiques (locaux, distants, de bureautique, de messagerie, etc.), les réseaux et vecteurs de communication (internet, téléphone, télécopie, etc.),
- les dispositifs de sécurité (contrôle d'accès, chiffrement, authentification forte, haute disponibilité, stockage et sauvegarde, etc.),
- les matériels, logiciels, applications et processus de traitement des données.

1.2. Droits et devoirs des utilisateurs

1.2.1. Dispositions générales

L'accès aux systèmes d'information de SOFIAP (poste de travail, messagerie, internet, téléphone, etc.) est fourni à l'*utilisateur* pour l'exercice de son activité professionnelle, sous le contrôle du responsable de son entité. Toutefois, un usage personnel est toléré dans le cadre d'une utilisation raisonnable.

La responsabilité pénale de l'*utilisateur* mais également celle de l'entreprise pouvant être engagées dans certaines circonstances, l'utilisateur doit exercer une vigilance toute particulière lors de l'utilisation des moyens fournis par SOFIAP. Ainsi, il est tenu de :

- **se conformer à l'ordre public et aux bonnes mœurs** : ne pas manipuler ou stocker sur les systèmes d'information de SOFIAP, des informations contraires aux bonnes mœurs et à l'ordre public (accès à des sites internet, stockage ou diffusion de fichiers, envoi de messages, etc.),
- respecter les **dispositions légales et réglementaires** en vigueur.

À ce titre, l'*utilisateur* veille, notamment, à respecter :

- **la propriété intellectuelle** : l'*utilisateur* ne doit pas réaliser de copies illicites d'éléments (logiciels, images, textes, musiques, etc.) protégés par un droit de propriété intellectuelle,
- **la protection des données à caractère personnel** : l'*utilisateur* respecte les dispositions légales et réglementaires en vigueur, relatives à la protection des données à caractère personnel, et à ce titre, informe Référent Informatique et Liberté (RIL) de SOFIAP, des traitements de données à caractère personnel qu'il serait amené à mettre en place dans le cadre de l'exercice de ses fonctions.

Il signalera notamment toute violation de données à caractère personnel conformément à la [procédure en vigueur](#)¹¹. Par ailleurs, il sera attentif au respect des durées de conservation des données dans le SI.

L'utilisateur contribue, à son niveau, à la sécurité des systèmes d'information. À ce titre, il se doit de :

- **utiliser** les systèmes d'information de manière **rationnelle et loyale** afin d'éviter leur saturation ou leur détournement,
- **se conformer aux procédures** techniques relatives à la mise en œuvre des ressources mises à sa disposition. En particulier, l'*utilisateur* ne doit jamais apporter volontairement des perturbations au bon fonctionnement des systèmes d'information, que ce soit par des manipulations indues de ressources ou par l'introduction de programmes malveillants tels que virus, logiciels espions...
- **signaler au support informatique** tout dysfonctionnement ou tout événement lui apparaissant anormal.

Enfin, l'utilisateur doit suivre les sessions de sensibilisation à la sécurité des systèmes d'information prévues par l'entreprise selon la fréquence définie.

1.2.2. Dispositions relatives à l'usage à titre personnel des ressources informatiques

L'utilisation des ressources informatiques à des fins autres que professionnelles est **tolérée** dès lors qu'elle reste **raisonnable**.

L'identification du caractère privé ou personnel d'une information relève de la responsabilité de l'*utilisateur*. Un fichier ou un courriel est considéré comme personnel :

- s'il est stocké dans un répertoire portant la dénomination particulière « PRIVE » ou « PERSONNEL », OU
- si l'élément contient la mention particulière « PRIVE » ou « PERSONNEL », dans son objet ou son nom.

Cette mention doit être exclusivement réservée aux données privées ou personnelles.

En l'absence de mention particulière « PRIVE » ou « PERSONNEL », un fichier ou un courriel est considéré comme professionnel.

L'usage à titre personnel des ressources informatiques mises à disposition par SOFIAP est encadré par les dispositions suivantes :

- l'usage doit être limité en volume et en durée de façon à n'affecter en rien le bon fonctionnement du système d'information,
- les fichiers personnels doivent être enregistrés dans un répertoire local non partagé,

¹¹ Il convient d'entendre par « violation », tout incident de sécurité, d'origine malveillante ou non et se produisant de manière intentionnelle ou non, ayant comme conséquence de compromettre l'intégrité, la confidentialité ou la disponibilité de données personnelles.

- lors d'une communication personnelle, *l'utilisateur* s'engage à s'assurer que le contenu ne présente aucune information liée à son activité professionnelle. Notamment, la signature professionnelle de *l'utilisateur* ne doit pas apparaître lors de l'utilisation à titre personnel de la messagerie.

L'utilisateur est informé qu'en cas de nécessité impérieuse (réquisition judiciaire, enquête interne ou risque ou événement particulier...), SOFIAP peut accéder à l'ensemble de ses fichiers et messages, y compris ceux identifiés comme « PRIVE » ou « PERSONNEL ». Dans le cas d'une enquête interne, la consultation des fichiers et messages identifiés comme « personnels » est réalisée en présence de *l'utilisateur* de la ressource ou celui-ci dûment appelé. En dehors de ces cas, une autorisation d'un juge peut être demandée.

1.2.3. Dispositions relatives à la protection des équipements

En protégeant les équipements qui lui sont confiés et en adoptant une attitude responsable, *l'utilisateur* contribue de manière essentielle à la sécurité des **informations placées sous sa responsabilité**.

Seuls les **équipements validés et répertoriés par SOFIAP** peuvent être installés et connectés aux réseaux internes et aux postes de travail informatiques de SOFIAP.

Chaque équipement (poste de travail, etc.) est livré avec une configuration standard qui couvre les besoins des *utilisateurs*. *L'utilisateur* ne doit **jamais modifier la configuration** des équipements mis à sa disposition par SOFIAP, notamment :

- il n'ajoute ni ne retire de composant matériel (disque dur, carte réseau, etc.) sans l'accord des services informatiques,
- il n'installe ni n'exécute de logiciel non référencé par les services informatiques. L'installation de tout logiciel doit être demandée aux équipes du support informatique qui évalueront le besoin et installeront le composant logiciel si nécessaire,
- il ne tente pas de modifier ou de désactiver les mécanismes de protection (logiciel antivirus, pare-feu, paramétrage des mots de passe, installation des correctifs de sécurité, etc.).

L'utilisateur est **responsable de la protection des équipements** mis à sa disposition. En particulier, il veille à :

- en cas d'absence, même momentanée, **verrouiller ou fermer toutes les sessions** en cours sur son poste de travail,
- utiliser les **moyens de protection disponibles** pour garantir la protection des équipements « mobiles » (ordinateurs portables, « smartphones », téléphones portables, tablettes numériques, disques dur externes, etc.) et de leurs accessoires : utilisation d'un câble antivol, rangement dans un tiroir ou une armoire fermant à clé, etc.,
- ne **pas laisser ses équipements sans surveillance** dans des lieux dont l'accès n'est pas contrôlé, et à faire preuve d'une vigilance particulière dans les lieux publics et les transports en commun,
- en cas de vol ou de perte, **appliquer sans délai les dispositions décrites** au § 1.2.10.3 intitulé « Vol ou perte d'une ressource » de la présente charte.

1.2.4. Dispositions relatives à la protection des informations

Les données des SI de SOFIAP auxquelles *l'utilisateur* a accès, sont la propriété de SOFIAP et ont une vocation professionnelle.

Afin de les protéger, *l'utilisateur* doit prendre toutes les mesures utiles, notamment respecter les règles suivantes :

- **assurer la confidentialité** des informations qui sont mises à sa disposition y compris dans les lieux professionnels, privés et surtout publics. Il veillera notamment à la protection de ses identifiants et mots de passe lors de leur saisie,
- **verrouiller son poste ou sa session de travail** dès qu'il s'absente de son poste de travail,
- **assurer la diffusion et le stockage** des informations dont il a connaissance, dans le cadre des règles données par sa hiérarchie, notamment en termes de confidentialité ; *l'utilisateur* s'assure que les informations confidentielles sont stockées et transmises de manière sécurisée, au moyen des outils mis à disposition par SOFIAP,
- **classifier les informations** aux niveaux adéquats comme l'exige la politique de sécurité des systèmes d'information en utilisant les niveaux : C0, C1, C2, C3 et C4,

Niveau	Confidentialité
0	INFORMATION PUBLIQUE (C0) L'information est accessible publiquement, après autorisation d'une entité habilitée à communiquer en dehors de SOFIAP, et ne nécessite aucune mesure de sécurité particulière.
1	INFORMATION INTERNE (C1) L'information a vocation à être diffusée librement mais uniquement au sein de SOFIAP à l'ensemble des collaborateurs et personnels sous contrat. Sa révélation à l'extérieur peut entraîner des conséquences mineures pour l'image et l'activité de SOFIAP.
2	INFORMATION RESTREINTE (C2) L'information n'est diffusable qu'à des utilisateurs issus de groupes ou de catégories de personnes identifiés. Cela peut correspondre à une équipe, à un groupe de travail, aux membres d'une même direction. Sa révélation à l'extérieur peut entraîner des conséquences significatives pour l'image et l'activité de SOFIAP.
3	INFORMATION CONFIDENTIELLE (C3) L'information n'est diffusable qu'à des utilisateurs explicitement désignés par leur poste et ayant le besoin d'en connaître ¹² . Sa révélation à d'autres personnes que celles désignées peut entraîner des conséquences critiques pour l'image et l'activité de SOFIAP.
4	INFORMATION SECRÈTE (C4) Il s'agit du niveau de classification le plus élevé et est réservé aux informations très sensibles rarement diffusées par écrit. L'information n'est diffusable qu'à un nombre très restreint d'utilisateurs nommément désignés. Sa révélation à l'extérieur peut entraîner les conséquences les plus graves pour l'image et l'activité de SOFIAP.

- il est interdit à l'utilisateur de charger, d'intercepter, de stocker, de lire, de copier, de détruire, de diffuser ou de modifier toute donnée ou fichier informatique qui lui a été communiqué par erreur et auquel il n'est pas censé avoir accès,
- dans le cas de la réception par erreur d'une information, l'utilisateur devra signaler l'erreur à l'expéditeur avant d'effacer l'information sauf contre-indication de ce dernier,
- en cas d'accès involontaire l'utilisateur ne devra pas prendre connaissance des informations et ne pas rester connecté à l'application. Il devra par ailleurs prévenir le support technique sans délai.

Pour éviter toutes fuites d'informations vers des réseaux extérieurs à SOFIAP, des règles figurent dans la politique de sécurité des systèmes d'information. Il est notamment rappelé qu'en cas de transfert de données depuis internet :

- une information de niveau C3 doit être obligatoirement chiffrée,
- la transmission d'une information de niveau C4 est interdite.

À son départ de SOFIAP (démission, départ à la retraite ou fin mission) ou lors d'un changement d'activité, l'utilisateur doit restituer à l'entreprise, l'ensemble des informations propriété de SOFIAP, sous forme intelligible, quel que soit leur support.

Il n'est pas autorisé à en faire une copie pour son usage personnel.

1.2.5. Dispositions spécifiques à l'accès aux systèmes d'information

L'utilisateur ne peut accéder aux informations que dans le cadre de ses activités professionnelles, définies par sa fonction au sein de SOFIAP et dans les limites fixées par les délégations accordées. À cette fin, des **droits d'accès aux systèmes d'information sont attribués à chaque utilisateur. Ils sont strictement personnels.**

Ces droits et habilitations peuvent être modifiés ou retirés à tout moment par SOFIAP. Toute autorisation prend fin lors de la cessation, même provisoire, de l'activité professionnelle.

L'utilisateur est responsable de l'utilisation des systèmes d'information réalisée avec ses droits d'accès. A ce titre, **il doit assurer la protection des moyens d'authentification** (badges, mots de passe, cartes d'authentification, etc.) qui lui ont été affectés :

- il **ne les communique jamais** à une tierce personne, y compris aux services informatiques, à ses collaborateurs ou à sa hiérarchie,
- il **respecte les règles** de complexité et de renouvellement des mots de passe. La bonne pratique recommande qu'un même mot de passe ne soit pas réutilisé pour des usages différents.

L'utilisateur ne peut accéder aux systèmes d'information qu'avec les identifiants qui lui ont été attribués. Toute connexion aux

¹² Règle qui limite le partage d'une information aux personnes qui justifient non seulement du niveau d'habilitation nécessaire mais aussi de la nécessité de la connaître.

systèmes d'information, transmission ou usage de données effectuées par l'utilisation des droits attribués à l'utilisateur est présumée effectuée par ce dernier, sauf preuve du contraire. L'utilisation **d'identifiants de tiers**, même disposant d'habilitations identiques, est **proscrite**.

L'utilisateur ne peut accéder qu'aux systèmes pour lesquels il est habilité. L'accès volontaire à un système d'information pour lequel l'utilisateur n'est pas habilité n'est pas autorisé. En cas d'accès involontaire, l'utilisateur ne doit pas prendre connaissance des informations et ne pas rester connecté à l'application.

La possibilité **d'accès à distance au réseau interne de SOFIAP** depuis l'internet est soumise à autorisation préalable. Lorsque cette autorisation est accordée, l'utilisateur doit respecter les règles d'usage et de sécurité qui lui ont été spécifiquement communiquées.

1.2.6. Dispositions spécifiques à l'utilisation de la messagerie électronique

Dans le cadre de son activité professionnelle, l'utilisateur ne doit utiliser que les moyens de communication (messagerie, messagerie instantanée, etc.) mis à sa disposition par SOFIAP conformément aux éventuelles dispositions spécifiques à son activité.

L'utilisateur est **responsable des messages qu'il émet**. À ce titre, il doit s'assurer :

- de protéger les informations envoyées par messagerie. Pour les messages non sécurisés par des moyens de chiffrement spécifiques, la sécurité offerte par la messagerie électronique standard est comparable à celle de l'envoi d'une carte postale,
- que le contenu des messages qu'il envoie ne porte pas atteinte à l'image ou à la réputation de SOFIAP,
- de ne pas modifier un message émanant d'un tiers avant de le rediffuser,
- de ne pas envoyer ni faire suivre de message non sollicité (« spam » ou « pourriels »), de message contenant des informations illicites ou offensantes, ou encore de message de type « chaîne »,
- de ne pas mettre en œuvre des fonctions d'envoi ou de redirection automatique des messages lui étant destinés vers une adresse de messagerie dont les conditions d'exploitation et de sécurité ne sont pas contrôlées par SOFIAP. En particulier, il est interdit de transférer ses messages professionnels vers ses messageries personnelles.

L'envoi de message à l'ensemble des utilisateurs de SOFIAP est interdit, sauf autorisation spécifique.

L'utilisateur fait preuve de **vigilance à l'égard des messages qu'il reçoit**. À ce titre, il reste **vigilant** :

- il n'ouvre pas les messages dont l'origine, l'objet ou le contenu est douteux. En cas de réception d'un tel message, il le signale aux services informatiques selon les procédures en vigueur. En particulier, il n'enregistre pas et n'ouvre pas les pièces jointes ou les liens présents dans un message suspect,
- il ne prend pas de décision importante à la seule vue d'un message électronique. La falsification des caractéristiques d'un courriel est une méthode classique dans le cadre de malversation, notamment celle de type « arnaque au président ». En cas de doute, il contacte l'émetteur du message ou à défaut, le support informatique pour s'assurer de l'authenticité et de la véracité des informations reçues.

En cas de réception par erreur d'une information, l'utilisateur signale l'erreur à l'expéditeur avant d'effacer l'information sauf contre-indication de ce dernier.

L'inscription sur des listes de diffusion est réservée à un usage strictement professionnel. En outre, l'utilisateur doit systématiquement vérifier lors de l'inscription qu'il existe une procédure de désabonnement.

L'usage de la messagerie à titre personnel est admis dans les conditions prévues au § 1.2.2.

1.2.7. Dispositions spécifiques à l'utilisation de l'internet

L'utilisateur accède uniquement à l'**internet** (ou un autre réseau externe) depuis les équipements mis à sa disposition par SOFIAP, au travers d'une solution d'accès autorisée par SOFIAP. Dans ce cadre, SOFIAP installe des filtres d'accès aux sites afin de limiter le périmètre des sites accessibles.

Le contournement des systèmes de filtrage et l'accès à des sites filtrés sont strictement interdits. **En cas d'accès accidentel à un site internet illégal ou non autorisé par SOFIAP**, l'utilisateur doit se déconnecter immédiatement de ce site.

L'utilisateur ne doit **jamais communiquer ses coordonnées professionnelles**, en particulier son adresse électronique, sur des sites sans rapport avec son activité professionnelle ou dont l'image est incompatible avec celle de SOFIAP.

L'utilisateur ne doit pas réutiliser de mots de passe personnels dans un cadre professionnel, et inversement.

La responsabilité pénale de l'utilisateur mais également celle de l'entreprise pouvant être engagée dans certaines circonstances, il est rappelé que l'utilisation d'internet doit être conforme aux dispositions générales décrites dans l'article

1.2.1. A ce titre, tout accès à des sites illicites, notamment des sites pédophiles, révisionnistes ou incitant à la haine, est formellement interdit.

Il est rappelé que l'usage d'internet à **titre personnel** est admis dans les conditions prévues au § 2.2.2. L'utilisateur est informé que SOFIAP met en place :

- des dispositifs de **surveillance** pour protéger les systèmes d'information contre toutes formes de menaces propagées par l'internet. Dans ce cadre, SOFIAP conserve la totalité des traces d'accès à internet pendant une durée d'un an. Elle les utilise dans le cadre des réquisitions judiciaires et des enquêtes internes.
- des dispositifs de détection d'accès aux sites interdits par la loi et ceux contraires à l'ordre public et aux bonnes mœurs.

1.2.8. Dispositions relatives à l'utilisation de la téléphonie

La mise à disposition de services de communications téléphoniques au sein de SOFIAP est destinée à satisfaire les besoins professionnels.

Néanmoins, il est rappelé que l'utilisation de la téléphonie à **titre personnel** est admise dans les conditions prévues au § 1.2.2.

L'utilisateur doit rester vigilant dans l'utilisation des réseaux téléphoniques publics fixes ou mobiles, la confidentialité des échanges n'étant pas garantie sur ces réseaux.

1.2.9. Dispositions relatives aux équipements mobiles

Dans la présente charte, le terme « équipements mobiles » couvre :

- les postes de travail nomades (ordinateurs portables) mis à disposition par SOFIAP, quelle que soit leur utilisation : utilisation bureautique classique, accès à des applications « métier », conduite d'opérations d'administration ou de supervision informatique, développement informatique, etc.,
- les téléphones mobiles communicants, « smartphones », tablettes numériques, etc.,
- les supports de stockage externe (clés USB, disques durs externes, CDROM, DVDROM, etc.).

Seuls les équipements mobiles **validés et répertoriés par SOFIAP** peuvent être installés et connectés aux systèmes d'information de SOFIAP (réseaux internes, accès distants, postes de travail informatiques, smartphone...).

Responsabilité des utilisateurs en situation de nomadisme

Les *utilisateurs* d'équipements mobiles doivent appliquer l'ensemble des dispositions précédemment exposées.

De plus, ils doivent être conscients des risques renforcés dans le cadre d'une utilisation nomade (hors des locaux de SOFIAP : à domicile, dans un hôtel, lors d'une conférence, dans les transports en communs, dans un véhicule, dans un restaurant, un café, ou dans tout autre lieu considéré comme public) :

- le risque de vol d'équipement :
l'utilisateur doit être particulièrement attentif à l'application des dispositions relatives à la protection des équipements décrites au § 1.2.3,
- le risque d'interception de données :
 - le poste informatique ne doit pas être connecté à des réseaux autres que ceux maîtrisés par SOFIAP, autrement qu'au travers des solutions de nomadisme mises à disposition par SOFIAP. Ces solutions de nomadisme définissent notamment les procédures à appliquer pour se connecter en environnement public ou privé, à l'aide d'un point d'accès internet public ou personnel, fixe ou mobile,
 - l'utilisateur doit prendre toutes les précautions utiles lors de l'utilisation des ressources informatiques dans les lieux publics pour éviter les indiscrétions. L'environnement de travail (orientation de l'écran, isolation de la zone de travail, ...) doit permettre de minimiser les risques de capture visuelle ou auditive de l'information par des tiers,
 - l'utilisateur doit privilégier en situation de nomadisme depuis son poste de travail LBP, les connexions sur le réseau 4G/5G et éviter de se connecter aux réseaux publics WIFI,
 - les informations classifiées « confidentielles » ou « secrètes » au sens de la « Charte de gestion de l'information sensible » établie par SOFIAP ne doivent pas être consultées lorsque l'environnement ne permet pas d'assurer que des personnes non autorisées ne pourront pas capturer ces informations,
- les risques liés à la non mise à jour des dispositifs de lutte contre les programmes malveillants.

En cas de possession d'un ordinateur portable, il est impératif de le connecter régulièrement au réseau informatique de SOFIAP pour s'assurer de la bonne mise à jour de sa configuration.

Utilisation individuelle des équipements mobiles

L'utilisation d'un équipement mobile (poste de travail nomade, assistant numérique personnel, téléphone mobile communicant, etc.) est individuelle et **ne doit pas être partagée** avec d'autres *utilisateurs*, sauf autorisation spécifique.

Certains cas d'utilisation partagée sont tolérés, en particulier dans le cadre d'opérations de support (par exemple les portables d'astreinte). L'équipement mobile doit alors être sous la responsabilité d'un unique propriétaire désigné.

1.2.10. Comportement en cas d'incident

1.2.10.1. Devoir général d'alerte

Il est du devoir de chaque *utilisateur* d'alerter sa hiérarchie, et/ou le déontologue si nécessaire, ainsi que son correspondant sécurité des systèmes d'information (ou à défaut le responsable de la sécurité des systèmes d'information) en cas de suspicion ou de constatation d'événements pouvant porter atteinte à la sécurité des systèmes d'information de SOFIAP.

Pour illustrer ces situations, dont la diversité suppose de la part de l'utilisateur attention et discernement, on citera :

- l'existence d'informations confidentielles sur des répertoires partagés non appropriés ou sur des serveurs ou services internet non sécurisés,
- l'existence de contenus à caractère offensant,
- la mauvaise application constatée de règles de sécurité,
- la présence de personnes non autorisées dans des zones de travail,
- les documents « abandonnés » contenant des informations confidentielles,
- toute violation de données à caractère personnel,
- toute tentative subie d'extorsion d'information.

1.2.10.2. Attaque par code malveillant ou intrusion sur le poste de travail

Sous l'appellation de « code malveillant » se trouvent les virus, les vers, les chevaux de Troie, les « ransomwares », etc.

Une intrusion sur le poste de travail peut se traduire par un comportement anormal du matériel ou des alertes des dispositifs de sécurité (alerte émise par le logiciel anti-virus, alerte du firewall applicatif).

En cas de suspicion ou de constatation de :

- tentative d'accès ou d'accès aux équipements qui lui sont confiés par SOFIAP, à son poste de travail ou à son terminal,
- intervention sur ses fichiers ou ses données,
- tout dysfonctionnement ou tout événement lui apparaissant anormal,
- alertes des dispositifs de sécurité (alerte émise par le logiciel anti-virus, alerte du firewall applicatif),

... sans tenter de résoudre lui-même l'incident, l'utilisateur doit, dans tous les cas :

- isoler le matériel : déconnecter le matériel du réseau de l'entreprise (connexions filaire et sans-fil),
- prévenir le support informatique qui prend les dispositions nécessaires pour traiter l'incident. L'utilisateur doit alors se conformer à ses consignes.

1.2.10.3. Vol ou perte d'une ressource

En cas de vol ou de perte d'une ressource, l'*utilisateur* doit dans les meilleurs délais prévenir :

- le support informatique pour le blocage des accès distants utilisés sur le matériel,
- son supérieur hiérarchique et ainsi que son correspondant sécurité des systèmes d'information (ou à défaut le responsable de la sécurité des systèmes d'information) ainsi que son référent informatique et liberté (RIL) ou le DPO délégué, en transmettant :
 - le descriptif des circonstances de la perte ou du vol,
 - l'inventaire des données (notamment des données à caractère personnel) qui étaient présentes sur le matériel avec leur niveau de sensibilité et leur niveau de protection au moment de la perte ou du vol.

1.3. Contrôles et collecte d'informations

Dans le respect des principes de transparence et de proportionnalité, à des fins de sécurité et de vérification du bon accès et usage des ressources, ainsi que du bon fonctionnement de ses systèmes d'information, SOFIAP met en place et assure le bon fonctionnement de systèmes de surveillance des usages, de filtrage et de contrôle (pare-feu, systèmes de contrôle des accès, antivirus, sonde de détection d'intrusion, Endpoint Detection and Response (EDR), filtrage des supports amovibles (USB), Contrôle Web, Data Loss Prevention (DLP), analyse forensic, collecte/corrélation des journaux d'événements, audit de conformité, Cyber Threat Intelligence (CTI), etc.).

Dans ce contexte, l'utilisateur est informé que les **traces** suivantes **peuvent être conservées**, sur une durée de douze mois et être communiquées dans le cadre des réquisitions judiciaires, administratives ou utilisées dans le cadre des enquêtes internes et des procédures disciplinaires :

- l'ensemble des contenus ou services auxquels l'utilisateur a eu accès sur l'internet ou les intranets de SOFIAP,
- de façon générale, l'ensemble des informations liées aux accès/connexion ou tentative d'accès/connexion à tout réseau de communication interne ou externe à partir des ressources,
- l'ensemble des informations liées aux accès à tout matériel (serveurs, imprimante, etc.), logiciel (applicatifs, etc.) ou donnée (fichiers, etc.) auxquels a accédé le compte de l'utilisateur,
- l'ensemble des informations liées à l'utilisation des services de messagerie électronique,
- les journaux (logs) ou traces diverses permettant de détecter, de circonscrire, d'empêcher ou de prouver l'existence ou la survenance d'incidents de sécurité, de malveillance et ou de fraudes informatiques.

L'utilisateur est informé que SOFIAP met en place des dispositifs de contrôles :

- portant notamment sur la volumétrie ou la fréquence des connexions à des sites internet, des services web, des messageries ou plus globalement de l'utilisation des ressources des systèmes d'information de SOFIAP,
- sur les équipements qu'elle fournit. Ces contrôles peuvent nécessiter la saisie de ces équipements.

L'utilisateur ne doit en aucun cas empêcher, tenter de contourner ou gêner le fonctionnement normal de ces contrôles.

Au besoin et en fonction du résultat des contrôles opérés, l'utilisation des ressources matérielles et logicielles, les services accédés (site, etc.) ainsi que les échanges, quels que soient leur nature ou leur objet, effectués via les systèmes d'information de SOFIAP peuvent notamment être limités ou interdits sans préavis ni information.

1.4. Sanctions

Le non-respect de la présente charte par l'utilisateur constitue une faute professionnelle, et peut entraîner, à son encontre, l'application d'éventuelles sanctions disciplinaires, de manière appropriée et proportionnée, conformément à l'échelle des sanctions prévues par le règlement Intérieur, sans préjudice de l'engagement de sa responsabilité civile et/ ou pénale en cas de commission ou de tentative de commission d'infraction, en tant qu'auteur ou complice. S'il s'agit d'un prestataire ou d'un intérimaire, la société-prestataire ou la société d'intérim sera notifiée du non-respect de la présente charte pour action.

Annexe 2 : Charte administrateur des moyens informatiques

1.5. Préambule

Les systèmes d'information constituent pour SOFIAP une ressource stratégique indispensable à la conduite de ses activités et à la satisfaction de ses clients. Ces systèmes d'information sont exposés à de nombreux risques en termes de sécurité et encadrés par des exigences légales, réglementaires et contractuelles de plus en plus strictes.

Dans ce contexte, une politique de sécurité des systèmes d'information a été définie par SOFIAP. La présente charte, élément de cette politique, a été établie dans le but de préciser les rôles et responsabilités des *administrateurs informatiques*.

Dans le présent document, le terme « **administrateur informatique** » ou « **administrateur** » désigne tout acteur quelle que soit sa fonction, qui a pour mission d'assurer le bon fonctionnement et la sécurité des ressources des systèmes d'information supports des activités de SOFIAP placées sous sa responsabilité (applications, serveurs, équipements réseaux, dispositifs de sécurité, bases de données, postes de travail utilisateurs et équipements bureautiques, messagerie, etc.).

Afin de conduire les actions quotidiennes d'administration et d'exploitation informatique afférentes à sa mission (paramétrage, configuration, supervision, maintenance, évolution, support, etc.), l'administrateur est doté de **droits d'accès spécifiques** sur les ressources des systèmes d'information sous sa responsabilité.

Compte tenu du niveau de ces droits d'accès spécifiques, la présente charte définit les pouvoirs et les devoirs des *administrateurs informatiques* en termes de sécurité des systèmes d'information. Elle s'inscrit dans une démarche d'information, de **sensibilisation** et de **responsabilisation**. Elle précise les règles et précautions que chacun d'entre eux doit respecter, afin de garantir une gestion licite, fiable et sécurisée des systèmes d'information supports des activités de SOFIAP.

La présente charte complète les dispositions de la « charte utilisateur des moyens informatiques de SOFIAP » applicable à ces personnels en tant qu'utilisateurs des systèmes d'information.

Les principes développés dans le présent document s'appliquent à tous les collaborateurs de SOFIAP, CDI, CDD, stagiaire, alternant, intérimaire, ainsi qu'à tout postier agissant « au nom et pour le compte » de SOFIAP et également aux intérimaires, consultants et autres prestataires de services.

1.6. Administrateurs informatiques

L'*administrateur* a pour mission d'assurer le bon fonctionnement et la sécurité des systèmes d'information supports des activités de SOFIAP qui sont placés sous sa responsabilité.

Il a un rôle de confiance. Sa démarche doit être impartiale et ses actions menées dans le cadre strict de sa mission.

1.6.1. Les pouvoirs de l'administrateur informatique

Dans l'exercice de ses fonctions, l'*administrateur* est susceptible d'avoir accès à tout ou partie des ressources des systèmes d'information afin de prendre toute disposition nécessaire à leur bon fonctionnement et leur sécurité.

Dans ce cadre, il peut être amené à :

- procéder à des vérifications fonctionnelles ou techniques sur les fichiers, annuaires, bases de données, la messagerie, les connexions à Internet, les fichiers de journalisation, etc., afin de déceler toute anomalie ou incident qui pourrait porter atteinte au bon fonctionnement ou à la sécurité des systèmes d'information,
- prendre l'ensemble des mesures techniques adéquates afin de :
 - maintenir ou de rétablir la sécurité des systèmes d'information,
 - conserver les éléments de preuve de toute anomalie, de tout incident de sécurité ou abus d'utilisation des systèmes d'information susceptibles de porter atteinte à leur bon fonctionnement, à leur confidentialité, à leur intégrité ou à leur traçabilité.

Les limites de l'intervention de l'administrateur sont fixées par :

- les lois et réglementations en vigueur,
- le code de conduite de SOFIAP qui comprend la « charte utilisateur des moyens informatiques » et la présente charte,
- sa fiche de poste et/ou le contrat de travail qui définit ses missions,
- l'encadrement contractuel de son intervention pour les prestataires ou la convention de stage ou d'intérim,
- les instructions de ses supérieurs hiérarchiques.

En aucun cas, il ne peut être contraint à enfreindre la loi.

1.6.2. Devoirs de l'administrateur informatique

L'*administrateur* est tenu à des **obligations strictes** en matière de **confidentialité**, mais également à un devoir de contribution à la sécurité des ressources.

Il doit, en toutes circonstances, faire preuve de **conscience professionnelle**, de **précaution** et de **rigueur** et agir **strictement dans le cadre de ses fonctions** : son action et ses accès doivent notamment être justifiés par les stricts besoins de sa mission.

1.6.2.1. Confidentialité

L'*administrateur* ne prend connaissance des informations contenues dans les systèmes d'information ou n'y donne accès que dans le cadre de ses missions et dans le **respect des procédures** internes formalisées.

Les informations des systèmes d'information de SOFIAP, auxquelles l'*administrateur* a accès, sont la propriété de SOFIAP et ont une vocation professionnelle. Afin d'en assurer la confidentialité, l'*administrateur* se conforme à la « charte utilisateur des moyens informatiques » et applique les règles relatives à la protection des informations qui y sont énoncées.

L'*administrateur* qui doit manipuler des fichiers s'engage à **s'abstenir de prendre connaissance** de leur contenu en dehors du strict exercice de sa mission.

L'*administrateur* ne doit **pas faire état des informations** qu'il peut être amené à connaître dans le cadre de ses fonctions. Il est tenu à une obligation de confidentialité sur ces informations.

Toute **copie** de toute information ou donnée recueillie dans ce cadre pour des motifs non liés aux missions de l'*administrateur* est **strictement prohibée**.

L'*administrateur* ne donne pas accès à des informations **sans l'autorisation formelle** de leur propriétaire (maîtrise d'ouvrage, instance habilitée, ...).

Les données à caractère personnel qui sont classées (C3) devront faire l'objet d'une attention et d'une protection particulière.

Par ailleurs, il ne prend pas connaissance des contenus relevant manifestement de l'usage à titre personnel des ressources informatiques et n'autorise personne à y accéder. Ainsi, tous les fichiers ou courriels contenant la mention « PRIVE » ou « PERSONNEL », dans leur objet ou leur nom, ou stockés dans un répertoire comportant cette dénomination, seront considérés comme étant « personnels ».

Dans le cas d'une enquête interne, la consultation des fichiers et messages identifiés comme « personnels » peut être demandée par le déontologue, elle doit alors être réalisée en présence de l'utilisateur de la ressource ou celui-ci dûment appelé. En dehors de ces cas, une autorisation d'un juge doit être obtenue préalablement.

1.6.2.2. Protection et utilisation appropriée des droits d'accès

L'*administrateur* protège l'utilisation des comptes et droits d'accès qui lui ont été attribués.

Chaque **identifiant** et chaque **authentifiant** (mot de passe, « token », carte, ...) associés à ces comptes est accordé de manière **nominative et personnelle**. Ils ne peuvent être communiqués, même sous contraintes opérationnelles fortes.

Toute demande pour que l'*administrateur* bénéficie de droits d'accès aux ressources informatiques doit être soumise à l'instance habilitée à cette fin. Dans tous les cas, l'*administrateur* doit faire la demande de droits d'accès auprès du son supérieur hiérarchique.

Il est interdit à l'*administrateur* d'utiliser des éléments de connexion (identifiant/authentifiant) qui ne lui ont pas été officiellement attribués.

Le fait de permettre l'accès, l'utilisation ou l'administration des systèmes d'information à quiconque en utilisant les droits d'accès de l'*administrateur* est proscrit. La responsabilité de l'*administrateur* pourra être engagée en cas d'action malveillante effectuée à l'aide de ses éléments de connexion.

Le cas échéant, il maintient secret, trace et limite au strict besoin fonctionnel l'utilisation des comptes de services qui ont pu lui être attribués.

En son absence, il sécurise, par le biais des protections disponibles, l'accès à son poste de travail ou à tout autre moyen informatique le reliant au système d'information.

L'*administrateur* engage sa responsabilité sur l'utilisation raisonnable et appropriée de ses droits d'accès.

Il **n'abuse pas de ses droits d'accès**, et limite ses actions aux ressources informatiques dont il a la charge, dans le respect de la finalité de sa mission. En particulier, il ne modifie les configurations et les droits d'accès que dans le respect de procédures d'administration ou d'exploitation définies.

L'utilisation des droits d'accès spécifiques qui lui ont été attribués doit être restreinte à la seule exécution de la mission qui lui est confiée. Si certains droits d'accès offrent techniquement, des possibilités plus larges que celles nécessaires à sa mission, il est de son devoir de ne pas outrepasser les limites des actions liées à sa mission.

Il utilise les outils d'administration et notamment ceux de télémaintenance dans le strict respect des procédures existantes et ne se connecte pas à un poste de travail d'un utilisateur sans autorisation formelle de celui-ci.

Il **ne contourne pas les procédures de sécurité établies**, et en particulier ne désactive pas de sa propre initiative les mécanismes de traçabilité, et ne porte pas atteinte à l'intégrité des fichiers de journalisation, sauf si le respect des procédures opérationnelles liées à l'administration des ressources applicables l'exige.

Dans le cadre de ses activités, par exemple lors d'une astreinte, l'*administrateur* peut être amené à réaliser des interventions à distance sur les systèmes d'information. Ces interventions doivent être régies par des procédures strictes et documentées, notamment en termes de nature des travaux à mener et de plages horaires d'intervention.

Les comptes d'accès attribués à l'*administrateur* disposant de droits d'accès élevés sur les systèmes ne doivent être utilisés que pour des actions « d'administration ». Les actions relevant de l'usage standard des ressources du système d'information (consultation de messagerie, navigation Internet, accès aux applications en tant qu'utilisateur...) doivent être réalisées avec le compte utilisateur qui lui a été attribué à cet effet.

Quand une personne dans le cadre de ses fonctions sur une application doit effectuer à la fois des actions métier et des actions d'administration, elle doit le faire en utilisant des comptes différents (dont un compte d'administration dédié).

Pour tous les administrateurs qui en disposent, les actions d'administrations sont réalisées à partir d'un poste de travail sécurisé dédié aux actes d'administration (poste SIA). Son usage peut être obligatoire pour certaines catégories d'applications.

1.6.2.3. Respect de la « politique de sécurité des systèmes d'information du groupe La Banque Postale »

Dans l'exercice de ses missions, l'*administrateur* veille à respecter et faire respecter la politique de sécurité des systèmes d'information dont fait partie la « charte utilisateur des moyens informatiques de SOFIAP » ainsi que la présente charte, et notamment :

- il n'utilise que des logiciels faisant partie des standards approuvés par SOFIAP dans le cadre de la conduite de sa mission et vis-à-vis des ressources à sa charge. L'installation de tout logiciel doit être validée par son responsable hiérarchique,
- il ne connecte ni n'utilise de périphériques de stockage de données (clés USB, ou tout autre dispositif utilisé dans ce but) ou plus largement de tout élément matériel étranger à SOFIAP, afin d'éviter toute introduction de virus ou autre code malveillant,
- il respecte en tant qu'utilisateur les dispositions de la « charte utilisateur des moyens informatiques ».

1.6.2.4. Devoir d'alerte

Tout *administrateur* doit **informer** sa hiérarchie, et/ou le déontologue si nécessaire, ainsi que son correspondant sécurité des systèmes d'information (ou à défaut le responsable de la sécurité des systèmes d'information) ainsi que le DPO délégué ou le RIL de l'entité dès lors qu'il :

- constate ou suspecte un dysfonctionnement des ressources des systèmes d'information,
- découvre ou a connaissance de toute faille, événement ou incident de sécurité,
- identifie ou soupçonne un usage des ressources des systèmes d'information non conforme à la politique de sécurité des systèmes d'information de SOFIAP.

Il ne prend pas ses consignes d'une personne non identifiée et fait remonter auprès de son responsable hiérarchique toute requête lui paraissant inappropriée.

1.6.2.5. Sensibilisation à la sécurité informatique

L'administrateur doit suivre les sessions de formation à la sécurité des systèmes d'information prévues par l'entreprise selon la fréquence définie.

1.7. Traçabilité et Contrôle

Dans le respect des principes de transparence et de proportionnalité, à des fins de sécurité et de vérification du bon accès et usage des ressources, ainsi que du bon fonctionnement des systèmes d'information de SOFIAP, des systèmes de surveillance des usages, de filtrage et de contrôle sont mis en place.

Les *administrateurs* sont informés que les **traces** d'actions suivantes réalisées à partir des comptes d'administration sont **conservées** sur une durée de douze mois :

- l'ensemble des contenus ou services accédés sur l'internet ou sur l'intranet de SOFIAP,
- l'ensemble des informations relatives accès/connexion ou tentative d'accès/connexion à tout réseau de communication interne ou externe,
- l'ensemble des informations relatives aux accès à tout matériel (serveurs, imprimante, etc.), logiciel (applicatifs, etc.) ou donnée (fichiers, etc.),
- l'ensemble des informations relatives à la gestion des services de messagerie électronique ainsi que les modifications de paramétrage et de configuration des ressources des systèmes d'information,
- les journaux (logs) ou traces diverses permettant de détecter, de circonscrire, d'empêcher ou de prouver l'existence ou la survenance d'incidents de sécurité, de malveillance ou de fraudes informatiques.

1.8. Sanctions

Le non-respect de la présente charte par l'*administrateur* constitue une faute professionnelle et peut entraîner, à son encontre, l'application d'éventuelles sanctions disciplinaires, de manière appropriée et proportionnée, conformément à l'échelle des sanctions prévues par le Règlement Intérieur, sans préjudice de l'engagement de sa responsabilité civile et/ou pénale en cas de commission ou de tentative de commission d'infraction, en tant qu'auteur ou complice.

S'il s'agit d'un prestataire ou d'un intérimaire, la société-prestataire ou la société d'intérim sera notifiée du non-respect de la présente charte pour action.

sofiap.fr

SOFIAP (Société Financière pour l'Accession à la Propriété), SA à Directoire et Conseil de surveillance au capital de 68 137 755 € - 64 rue de Saintonge - 75003 Paris - SIREN 391 844 214 RCS PARIS – IDU REP Papiers FR276343_03RYBR - immatriculée à l'ORIAS sous n° 07 025 372.