

Code de déontologie de CDC Informatique

Date d'entrée en vigueur 15/05/2026



Table des matières

Préambule	3
Les principes et les règles de déontologie	5
et de bonne conduite	5
Principe 1 : Respecter pleinement les obligations légales et réglementaires	6
Principe 2 : Respecter le devoir de réserve ainsi que les obligations de discrétion professionnelle et de probité.....	9
Principe 3 : Garantir la confidentialité	9
Principe 4 : Prévenir et gérer les conflits d'intérêts	10
Principe 5 : S'assurer que l'indépendance des collaborateurs ne puisse être remise en cause dans les relations avec les tiers.....	11
Principe 6 : Veiller à la primauté des intérêts des clients	12
Principe 7 : Respecter les règles de déontologie financière	13
Principe 8 : Appliquer les règles relatives à l'exercice des mandats sociaux.....	14
Principe 9 : Agir de manière loyale	15
Principe 10 : Protéger le patrimoine	15
Principe 11 : Veiller à une responsabilité sociale, sociétale et environnementale	16
Principe 12 : Mettre en place un dispositif d'alerte professionnelle.....	18
La « Fonction déontologie » et son organisation au sein	20
de CDC Informatique	20
Fonctions de la DAJCD CDC/service déontologie de la CDC et de la filière déontologie	21
Fonctions et organisation de la DMRCC ICDC en matière de déontologie	21
Diffusion des normes de déontologie	21
Formation et conseil aux collaborateurs	21
Comité de déontologie ICDC	22
Relation avec les autorités de supervision	22
Contrôle.....	22
Déclaration d'incidents	22
CE QU'IL FAUT RETENIR.....	24

Préambule

La Caisse des dépôts et consignations et ses filiales constituent un groupe public au service de l'intérêt général et du développement économique du pays. Le Groupe remplit des missions d'intérêt général en appui des politiques publiques conduites par l'État et les collectivités locales et peut exercer des activités concurrentielles¹ ».

Le groupe Caisse des Dépôts s'appuie sur une politique de responsabilité sociétale exigeante placée au cœur de ses priorités stratégiques.

La Caisse des Dépôts respecte les obligations légales et réglementaires qui s'imposent à elle du fait de son statut particulier. En matière de déontologie, elle vise l'exemplarité en s'inspirant des meilleures pratiques. Dans ce cadre, la Caisse des Dépôts met notamment en œuvre des dispositifs robustes visant à lutter contre la corruption, la fraude, le blanchiment de capitaux et le financement du terrorisme, à prévenir les conflits d'intérêts ainsi qu'à encadrer la déontologie financière.

Les principes du Code de déontologie de la Caisse des Dépôts sont transposés par CDC Informatique, en tant que *GIE* « in house » de la Caisse des Dépôts et Consignations, dans son propre Code de déontologie, objet de ce document.

Le présent Code s'applique à tous les collaborateurs de CDC Informatique. Est considéré comme un collaborateur au sens du présent Code de déontologie : toute personne de CDC Informatique ayant le statut de salarié, stagiaire, alternant, mandataire social, salarié mis à disposition de CDC Informatique et intérimaire

L'ensemble des processus qui permet à CDC Informatique d'honorer son objet social est décrit par des procédures incluant des dispositifs de contrôle interne.

Ce Code déontologique revêt un caractère préventif. Il a pour objectif de guider chaque collaborateur de CDC informatique dans la conduite à tenir lorsque des situations particulières peuvent rendre délicat l'exercice de ses fonctions. Le respect des obligations et des principes déontologiques relève de la responsabilité de chaque collaborateur.

Ledit Code rappelle également les dispositifs d'assistance et de signalement à la disposition des collaborateurs lorsque ces derniers sont confrontés, dans le cadre de leur mission, à des dysfonctionnements, des manquements, des malversations ou des fraudes, en complément des procédures d'alerte hiérarchique mises en place par CDC Informatique.

Il constitue un socle commun de principes et de règles de bonne conduite que chaque collaborateur a l'obligation de mettre en œuvre au quotidien. Des procédures d'application complètent, le cas échéant, les principes et les règles énoncés dans ce Code.

Chaque collaborateur de CDC Informatique s'engage à respecter les règles du Code qui lui sont applicables. En cas de manquement aux règles qui y sont édictées, CDC Informatique pourra prononcer des sanctions disciplinaires (Cf. Règlement Intérieur d'CDC Informatique), non exclusives d'éventuelles sanctions pénales que le collaborateur pourrait encourir.

¹ Article L.518-2 du Code monétaire et financier, modifié par la loi de modernisation de l'économie en 2008.

La présente version du Code de déontologie se substitue aux versions antérieures, mais ne se substitue pas aux dispositions législatives et réglementaires applicables conformément aux dispositions prévues au principe n°1 du présent Code.

Le service Déontologie de la Direction de la Maitrise des Risques, du Contrôle permanent, de la Conformité et de la Déontologie (ci-après « DMRCC ») veille au respect et à l'application du Code de déontologie et répond de toute question relative à la mise en œuvre dudit document et/ou de toute situation particulière. Pour davantage de précisions sur le rôle, les missions et l'organisation de ce service, il convient de se reporter à la seconde partie du présent Code intitulée « **La Fonction déontologie et son organisation au sein de CDC Informatique** », laquelle détaille les actions et modalités d'intervention du service Déontologie.

Les principes et les règles de déontologie et de bonne conduite

Principe 1 : Respecter pleinement les obligations légales et réglementaires

Les collaborateurs concourent au respect permanent des dispositions légales et réglementaires applicables à leur activité professionnelle.

Le Groupe Caisse des Dépôts déploie des dispositifs visant à lutter contre la fraude, la corruption, le blanchiment de capitaux et le financement du terrorisme ainsi qu'un dispositif visant à protéger les données à caractère personnel que CDC Informatique décline en fonction de ses spécificités.

Tout collaborateur de CDC Informatique est tenu d'observer strictement les dispositions applicables à son activité professionnelle et à son statut, qu'il s'agisse des obligations légales et réglementaires, des règles du présent Code, de l'usage des outils informatiques et de télécommunications, des instructions et des procédures édictées par l'autorité hiérarchique² et/ou tout canal d'information dûment établi.

Il est informé de ces dispositions par la hiérarchie³ ou par les moyens de communication propres à CDC Informatique. Il doit être particulièrement attentif aux règles et aux procédures susceptibles d'avoir une incidence directe sur son action quotidienne et sur les intérêts qui lui sont confiés.

Au regard de la sensibilité de ces sujets, toute entorse aux règles et procédures en vigueur expose en outre CDC Informatique à un risque de réputation particulièrement fort.

Libre concurrence

CDC Informatique et ses collaborateurs agissent dans le respect des règles afférentes à la commande publique, des pratiques commerciales et du droit de la concurrence, ce qui implique un traitement loyal des partenaires extérieurs, garantissant l'égalité de traitement, la transparence et le respect de la confidentialité des entreprises en compétition.

Lutte contre la corruption

A l'instar du Groupe Caisse des dépôts, CDC Informatique s'engage dans la lutte contre la corruption et les manquements à la probité avec une tolérance zéro face aux actes, tentatives et soupçons de corruption publique ou privée, active ou passive.

Il peut s'agir d'actes ou de faits survenant entre un collaborateur et un client, entre deux ou plusieurs collaborateurs, dans la relation avec un partenaire ou avec d'autres tiers⁴ en relations d'affaires ou utilisant les services de CDC Informatique.

Aussi, au titre des différents comportements à proscrire car susceptibles de caractériser des faits de corruption ou de trafic d'influence, les collaborateurs ne doivent pas accepter, solliciter ou offrir directement ou indirectement un- avantage indu⁵ ou la promesse d'un tel avantage à toute personne, privée ou publique dans le but d'obtenir un traitement de faveur ou d'influencer une négociation ou une relation d'affaires.

En outre, CDC Informatique fait preuve de vigilance dans l'octroi de subventions ou de dons à des tiers afin d'éviter tout fait ou acte de corruption.

² Le collaborateur « doit se conformer aux instructions de son supérieur hiérarchique, sauf dans le cas où l'ordre donné est manifestement illégal et de nature à compromettre gravement un intérêt public ». Le refus d'obéissance équivaut à une faute professionnelle. La subordination hiérarchique impose également de se soumettre au contrôle hiérarchique de l'autorité supérieure compétente et de faire preuve de loyauté dans l'exercice de ses fonctions. Le devoir d'obéissance impose enfin au collaborateur de respecter les lois et règlements de toute nature.

³ « Hiérarchie » fait référence au responsable hiérarchique du collaborateur, chargé notamment de l'évaluer ; le Code y fait référence en cas de survenance de situations pouvant porter à conflits d'intérêts ou dans le cas de l'exercice d'une activité professionnelle en dehors de la Caisse des dépôts ou de l'une de ses filiales.

⁴ Est considéré comme tiers au sens du présent Code, toute personne physique ou morale autre que CDC Informatique et ses collaborateurs

⁵ Par exemple versement ou réception d'une somme d'argent, de tout bien ou actif

La prévention et la détection des faits ou actes de corruption concernent tous les collaborateurs : chacun contribue à prévenir la corruption ou à y mettre fin lorsqu'il en a connaissance. Les collaborateurs signalent, sans délai, toute opération suspecte à leur hiérarchie qui en informe sans délai la Direction Générale, et le service Déontologie de la Direction de la Maitrise des Risques, du Contrôle permanent, de la Conformité et de la Déontologie (ci-après « DMRCC ») afin de permettre un traitement des cas, tentatives ou suspicions de corruption.

Ces situations peuvent également faire l'objet d'une alerte professionnelle telle que prévue au présent Code de déontologie.

Un collaborateur ne sera jamais sanctionné pour avoir refusé toute forme de corruption, même si cette décision a des conséquences commerciales défavorables.

En revanche, la participation d'un collaborateur à un acte de corruption est une faute professionnelle susceptible de sanctions disciplinaires, sans préjudice d'éventuelles poursuites ou condamnations judiciaires. La participation d'un partenaire à un acte de corruption doit se traduire par la rupture immédiate de la relation d'affaires.

Définitions ⁶
La corruption active : c'est la promesse, l'octroi ou l'offre, de tout avantage indu (pécuniaire ou autre) à toute personne, privée ou publique, dans le but d'obtenir un traitement de faveur (par action ou omission volontaire de cette personne) ou d'influencer une négociation ou une relation d'affaires. .
La corruption passive : c'est la sollicitation, la demande, la réception ou l'acceptation de tout avantage indu (pécuniaire ou autre) de la part de toute personne, privée ou publique, en contrepartie d'un traitement de faveur (par action ou omission volontaire de l'agent concerné ou de l'Entité) ou d'une influence sur une négociation ou une relation d'affaires
Le trafic d'influence actif est le fait par quiconque, de solliciter ou d'agréer, à tout moment, directement ou indirectement, des offres, des promesses, des dons, des présents ou des avantages quelconques, pour lui-même ou pour autrui, pour abuser ou avoir abusé de son influence réelle ou supposée en vue de faire obtenir d'une autorité ou d'une administration publique des distinctions, des emplois, des marchés ou toute autre décision favorable. Constitue le délit de trafic d'influence passif, le fait de céder aux sollicitations prévues à l'alinéa précédent ou de proposer, sans droit, à tout moment, directement ou indirectement, des offres, des promesses, des dons, des présents ou des avantages quelconques à une personne, pour elle-même ou pour autrui, pour qu'elle abuse ou parce qu'elle a abusé de son influence réelle ou supposée en vue de faire obtenir d'une autorité ou d'une administration publique des distinctions, des emplois, des marchés ou toute autre décision favorable.
Abus de confiance est le fait par une personne de détourner, au préjudice d'autrui, des fonds, des valeurs ou un bien quelconque qui lui ont été remis et qu'elle a acceptés à charge de les rendre, de les représenter ou d'en faire un usage déterminé.

⁶ Les peines encourues pour les différents schémas de corruption sont précisées aux articles 432-11 à 432-11-1 (corruption passive et trafic d'influence commis par des personnes exerçant une fonction publique), 433-1 à 433-2-1 (corruption active et trafic d'influence commis par les particuliers) et aux articles 445-1 à 445-2-1 (corruption passive et active des personnes n'exerçant pas une fonction publique) du Code pénal ; pour l'abus de confiance, il s'agit de l'article 314-1 du Code pénal.

Lutte contre la fraude

La fraude est entendue comme un acte intentionnel réalisé en utilisant des moyens déloyaux afin d'obtenir un consentement, un avantage matériel ou moral indu, ou réalisé avec l'intention d'échapper à l'exécution des lois et règlements. La fraude peut être interne ou externe. Les actes de fraude mettent particulièrement en risque les activités et les intérêts de CDC Informatique, de ses membres, de ses clients ou partenaires d'affaires.

Prévenir et lutter contre la fraude nécessite la vigilance de tous, à chaque instant. Les collaborateurs doivent être particulièrement vigilants face à toute opération suspecte ou situation atypique et les signaler, par écrit et sans délai à leur hiérarchie, afin de permettre un traitement adapté des cas, tentatives ou suspicions de fraude.

La fraude, comme tout comportement répréhensible, peut engager la responsabilité civile ou pénale du collaborateur qui la commet (notamment pour abus de confiance ou escroquerie).

Une fraude commise par un collaborateur en dehors des activités professionnelles mais qui se traduit par une atteinte aux intérêts de CDC Informatique est considérée comme une fraude interne.

CDC Informatique dispose d'une note d'organisation de la lutte contre la fraude distincte du présent Code et disponible sur l'intranet de CDC Informatique sur les pages dédiées à la Déontologie et dans le référentiel des processus et procédures.

Lutte contre le blanchiment de capitaux et le financement du terrorisme

N'étant pas un établissement financier, CDC Informatique n'est pas assujetti aux règles sur la lutte contre le blanchiment des capitaux et le financement du terrorisme.

Toutefois, CDC Informatique applique la politique LCB-FT du Groupe.

L'honorabilité des fournisseurs est à surveiller pour être conforme à ces politiques. Une procédure sur les diligences relatives à l'honorabilité des fournisseurs de CDC Informatique a été mise en place par CDC Informatique, est appliquée et est contrôlée. Cette procédure est disponible sur l'intranet de CDC Informatique dans le référentiel des processus et procédures.

Protection des données à caractère personnel

CDC Informatique met en œuvre une politique et un dispositif de protection des données à caractère personnel, conformément aux obligations légales et réglementaires, nationales et européennes en vigueur ainsi qu'aux délibérations et recommandations de l'autorité de contrôle (CNIL).

Ce dispositif s'inscrit notamment dans le cadre du Règlement (UE) 2016/679 du 27 avril 2016 (RGPD) et de la loi n°78-17 du 6 janvier 1978 modifiée dite « Informatique et Libertés ».

CDC Informatique a mis en place une organisation interne destinée à gérer les différentes problématiques posées par la protection des données personnelles et a désigné un(e) délégué(e) à la protection des données (DPO) conformément à l'article 37 du RGPD. Dans ce cadre, le DPO assure notamment la sensibilisation et la formation des collaborateurs, conseille le responsable de traitement et veille au respect des obligations prévues aux articles 24 à 39 du RGPD.

Chaque collaborateur doit veiller à respecter les obligations légales et réglementaires en matière de protection des données à caractère personnel.

Le collaborateur veille notamment à :

- n'accéder, ne gérer et ne traiter les données à caractère personnel qui lui ont été rendues accessibles que dans la mesure où c'est strictement nécessaire ;
- ne pas communiquer, sous quelque forme ou par quelque moyen que ce soit, les données à caractère personnel à des personnes qui ne sont pas expressément autorisées à y accéder ;
- limiter la collecte et le traitement aux seules données strictement nécessaires à la finalité poursuivie.

CDC Informatique dispose d'une procédure sur la gestion des données à caractère personnel distinct du présent Code et disponible sur l'intranet de CDC Informatique dans le référentiel des processus et procédures.

Principe 2 : Respecter le devoir de réserve ainsi que les obligations de discrétion professionnelle et de probité

En toutes circonstances, chaque collaborateur est tenu au devoir de réserve ainsi qu'à une obligation de discrétion⁷ professionnelle et de probité. En toutes circonstances, ils s'interdisent toute formulation ou action susceptible d'être qualifiée d'abusives pouvant porter atteinte à l'image et à la réputation de CDC Informatique.

La discrétion professionnelle couvre tous les faits, informations ou documents dont les collaborateurs ont connaissance dans l'exercice de leurs fonctions.

Le devoir de réserve est entendu comme l'obligation pour tous d'user de mesure, de retenue et de modération à l'occasion de l'expression publique de ses opinions.

Cette extériorisation d'opinions, notamment politiques, ne doit pas porter atteinte aux intérêts et à l'image de CDC Informatique ou du Groupe.

Une vigilance particulière est attendue dans les échanges avec l'extérieur, quel que soit le support utilisé (courriel, téléphone, tous les médias, y compris les réseaux sociaux) afin de ne pas nuire à CDC Informatique ou au Groupe. Toute diffusion non autorisée d'informations ou de données confidentielles est strictement interdite.

Sans préjudice des droits des représentants du personnel, les relations avec le public et les médias sont du ressort de la direction Générale de CDC Informatique, et de la Direction de la communication.

Toute intervention publique ou toute publication d'un collaborateur de CDC Informatique au nom et/ou pour le compte de CDC Informatique est soumise par ce collaborateur à l'autorisation préalable de sa hiérarchie et du Directeur général.

Principe 3 : Garantir la confidentialité

La confidentialité est indispensable pour garantir la protection des intérêts de CDC Informatique, de ses collaborateurs, de ses membres, de ses clients, de ses fournisseurs, et partenaires.

Cette obligation découle notamment de l'article L.1222-1 du Code du travail relatif à l'exécution de bonne foi du contrat, des dispositions relatives au secret des affaires (articles L151-1 et suivants du Code de commerce), au secret professionnel (article 226-13 du Code pénale) et des engagements contractuels souscrits avec les partenaires et prestataires de CDC informatique.

La confidentialité est le fait de s'assurer que l'information n'est accessible qu'aux personnes habilitées à y avoir accès. En toutes circonstances, une obligation de confidentialité s'applique à chacun.

⁷ La discrétion désigne une attitude qui veille à ne pas gêner les autres

D'une manière générale, sont jugées comme confidentielles, par défaut et par précaution, toutes les informations, quelle qu'en soit la forme et la nature, relatives à CDC Informatique, ses collaborateurs, ses clients (membres et non membres) et notamment les informations :

- relevant du secret professionnel⁸, du secret bancaire et de tout autre secret protégé par la loi, en ce compris le secret des affaires au sens des articles L 151-1 et suivants du Code de commerce ;
- relatives à un contrat ou une convention ;
- dont la diffusion est de nature à porter préjudice aux personnes ou entités visées ci-dessus ;
- ayant un caractère personnel ou médical relatives à une situation individuelle ;
- réputées privilégiées (telles que définie dans la suite de ce document) concernant CDC Informatique, ses clients (membres et non membres) ses partenaires, ses contreparties et ses collaborateurs,
- Et, dans tous les cas, les informations dites confidentielles ou secrètes conformément à la politique de classification de l'information de CDC Informatique.

Ainsi, au-delà des réglementations spécifiques (protection des données personnelles, secret protégé par une loi, etc.), chacun doit rester attentif à protéger l'information dont il dispose pour des besoins professionnels afin d'en éviter un usage inapproprié ou malveillant.

En particulier, les collaborateurs doivent s'assurer que les informations confidentielles ne circulent qu'entre les personnes habilitées à y avoir accès et exclusivement pour les besoins professionnels. Outre le fait de ne pas utiliser ces informations à des fins personnelles, ils doivent être attentifs à ne pas les divulguer, notamment lorsqu'il s'agit d'opérations en projet.

Chaque collaborateur veille également à la sécurité des systèmes d'informations et au respect des politiques internes de cybersécurité. Il s'interdit notamment d'utiliser des supports non-sécurisés, des outils numériques externes ou des outils de communication non approuvés par CDC informatique.

La confidentialité s'applique en toutes circonstances et à tous les types de médias, y compris les canaux de communication comme les réseaux sociaux.

Au sein de CDC Informatique, la confidentialité des informations peut être renforcée, de manière formelle, au cas par cas, en fonction des nécessités des missions, sur validation de la hiérarchie et/ou du/de la Directrice DMRCC.

La Charte d'utilisation des ressources des systèmes d'informations de CDC Informatique fixe les règles et les principes de confidentialité.

L'obligation de confidentialité perdure après la cessation des fonctions au sein de la CDC Informatique. Toute violation de cette obligation peut donner lieu à des sanctions disciplinaires et, le cas échéant, à des poursuites civiles ou pénales.

L'information privilégiée relative à la déontologie financière relève de dispositions spécifiques détaillées au principe 7 du présent Code de déontologie.

Principe 4 : Prévenir et gérer les conflits d'intérêts

Dans l'exercice de leurs fonctions, les collaborateurs agissent en toute objectivité, avec discernement et probité en vue de prévenir et de gérer les conflits d'intérêts.

⁸ Secret professionnel : en vertu de l'article 226-13 du Code pénal, la révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15 000 euros d'amende.

L'obligation n'est pas absolue : la révélation des secrets acquis est parfois permise, voire obligatoire. L'article 226-13 du Code pénal n'est pas applicable dans les cas où la loi impose ou autorise la révélation du secret.

De plus, selon l'article 45 de la convention d'entreprise : « Chaque collaborateur s'oblige, par son contrat de travail, à observer, d'une manière permanente vis-à-vis des tiers, un secret professionnel absolu, d'une part, sur les procédés employés et les résultats obtenus par la société, d'autre part, sur les renseignements concernant les clients de la société qu'il aurait été amené à connaître au cours de son travail. ».

Un conflit d'intérêts désigne une situation dans laquelle un collaborateur peut être amené à arbitrer directement ou indirectement, entre des intérêts réellement ou apparemment divergents et notamment entre son intérêt propre celui de CDC Informatique.

L'intérêt est entendu au sens large et il peut s'agir d'un intérêt matériel, immatériel ou financier.

Le conflit d'intérêts peut concerner chaque collaborateur, quelle que soit sa fonction. Il ne s'agit pas d'une situation répréhensible en soi ou d'une entorse aux règles applicables, mais elle peut être de nature à influencer ou paraître influencer l'exercice indépendant, impartial et objectif des fonctions.

Le collaborateur doit indiquer sans délai toute survenance de situation portant à conflit d'intérêt (potentiel ou avéré) dès lors qu'elle pourrait interférer sur les missions qui lui sont confiées. Notamment, les collaborateurs susceptibles d'utiliser ou de contracter avec un fournisseur ou un prestataire, ou de participer à un appel d'offre, doivent s'assurer que leur participation au processus de sélection du fournisseur ou prestataire ne serait pas de nature à générer un conflit d'intérêts.

Tout conflit d'intérêts est traité avec diligence.

Lorsqu'un collaborateur se trouve en situation de conflit d'intérêts, il le déclare par écrit à son responsable hiérarchique et le documente afin que la situation soit consignée dans un registre tenu par le service Déontologie de DMRCC. Lorsque ces faits lui sont signalés, le service Déontologie de DMRCC apporte au collaborateur concerné tous conseils concernant les mesures de prévention et de gestion à mettre en œuvre. Si nécessaire, le service Déontologie de DMRCC pourra demander un avis de la Direction des Ressources Humaines et un arbitrage du Directeur Général.

CDC Informatique dispose d'une procédure dédiée à la gestion des conflits d'intérêts, distincte du présent Code et disponible sur l'intranet de CDC Informatique dans le référentiel des processus et procédures.

Principe 5 : S'assurer que l'indépendance des collaborateurs ne puisse être remise en cause dans les relations avec les tiers

Cadeaux et avantages

CDC Informatique n'octroie pas de cadeaux ou avantages à des tiers dans le cadre de ses activités et attend de ses collaborateurs qu'ils refusent tout cadeau/avantage offert par des tiers au titre de leurs fonctions.

Les cadeaux ou avantages doivent être entendus comme tout bien matériel, tout service ou invitation reçu(e) ou octroyé(e) par un collaborateur au seul titre de ses fonctions.

Sont par exemple considérés comme cadeau/avantage :

- Tout objet ou toute somme d'argent numéraire ou dématérialisée (cartes cadeaux ou coffrets cadeaux) ;
- Tout service ou prestation gratuite habituellement commercialisé (ou toute réduction significative) ;
- Toute place de spectacles culturels et d'événements sportifs ;
- Toute invitation à déjeuner par un tiers ;
- Toute invitation à des voyages, week-end, séminaires et colloques pris en charge financièrement, partiellement ou totalement (frais d'inscription, transport et hébergement).

Les objets promotionnels⁹ de faible valeur (inférieure à 10 euros) qui participent de pratiques d'affaires courantes, ne sont pas considérés comme des cadeaux/avantages.

En cas de doute sur la nature d'un cadeau/avantage, il convient de saisir le service Déontologie de DMRCC.

⁹ Un objet promotionnel est défini comme un produit de faible coût utilisé par une entreprise pour promouvoir sa marque, ses produits ou ses services. Il est généralement personnalisé avec son logo ou le nom de l'entreprise à des fins marketing ou publicitaires.

Les modalités d'application et les exceptions à ce principe d'interdiction sont strictement énumérées et encadrées dans une procédure dédiée à la gestion des avantages et cadeaux, distincte du présent Code et disponible sur l'intranet de CDC Informatique dans le référentiel des processus et procédures.

Relation avec les fournisseurs et prestataires

CDC Informatique ne s'engage qu'avec les fournisseurs et prestataires référencés par le Service des Achats de CDC Informatique dans le cadre de l'application des règles de la commande publique.

CDC Informatique, au travers de son SPASER (Schéma de Promotion des Achats Socialement et Ecologiquement Responsables), oriente sa stratégie d'achats au service de 3 piliers du développement durable : social, environnement et développement économique.

Dans le cadre des règles de la commande publique, il est rappelé que CDC Informatique dispose de procédures permettant de choisir en toute transparence, loyauté, et égalité de traitement, le fournisseur dont les prestations seront le plus adapté à ses besoins (article L3 du Code de la commande publique).

Il est rappelé que le non-respect de ces règles est sanctionné pénalement et peut porter atteinte à la réputation de CDC Informatique. Chaque collaborateur doit donc être particulièrement attentif à leur respect.

De façon plus spécifique, les collaborateurs s'interdisent de contracter avec tout fournisseur ou prestataire proposant des conditions susceptibles d'aboutir à des facturations anormalement supérieures ou inférieures au prix de marché (par le biais par exemple de fractionnement d'achat, ou la multiplication des avenants).

Principe 6 : Veiller à la primauté des intérêts des clients

CDC Informatique s'assure de la protection de sa clientèle. Il en découle un devoir d'agir en conformité avec les intérêts des clients tout en veillant à préserver ceux de CDC Informatique. Ce principe découle du devoir général de loyauté et de bonne foi dans l'exécution des prestations conformément à l'article 1104 du Code civil.

Obligation de connaissance des clients

Les collaborateurs de CDC Informatique sont notamment tenus de recueillir l'ensemble des données utiles et nécessaires relatives à leurs clients afin notamment de leur fournir une information appropriée, pertinente et non trompeuse, leur précisant toujours l'étendue et la nature des risques liés à l'exécution des opérations effectuées à leur demande.

La collecte et le traitement des données sont réalisés conformément au RGPD et à la loi Informatique et libertés. Toute donnée est traitée de manière loyale, transparente et proportionnée aux finalités poursuivies.

La stricte confidentialité des informations les concernant doit être garantie.

Réclamations des clients

Une réclamation est une contestation, fondée ou non, exprimée oralement ou par écrit, par un client, portant sur la prestation délivrée par CDC Informatique et appelant la mise en œuvre d'un traitement (une réponse, une solution, une réparation).

Les réclamations des clients doivent être traitées avec diligence. Une réponse écrite et circonstanciée doit leur être adressée dans les meilleurs délais. La Direction de la Maîtrise des Risques, du Contrôle permanent et de la Conformité de CDC Informatique (DMRCC) est en copie des réclamations et des réponses aux réclamations.

Principe 7 : Respecter les règles de déontologie financière

Les collaborateurs ne peuvent réaliser et doivent refuser d'exécuter les opérations qui porteraient atteinte à l'intégrité des marchés. Ils sont tenus de refuser d'effectuer des opérations qui ne seraient pas conformes aux activités pour lesquelles ils sont mandatés et/ou à la réglementation et procédures internes qui leur sont applicables.

Définitions et principes généraux

Sont considérés comme des abus de marché les opérations d'initiés (utilisation d'information(s) privilégiée(s)) et la manipulation de marché.

Une *information privilégiée* est définie comme une information à caractère précis qui n'a pas été rendue publique, qui concerne, directement ou indirectement, un ou plusieurs émetteurs d'instruments financiers, ou un ou plusieurs instruments financiers, et qui, si elle était rendue publique, serait susceptible d'influencer de façon sensible le cours des instruments financiers concernés ou le cours d'instruments financiers dérivés qui leur sont liés.¹⁰

Une information est réputée précise si elle fait mention d'un ensemble de circonstances ou d'un événement qui s'est produit ou qui est susceptible de se produire et s'il est possible d'en tirer une conclusion quant à l'effet possible de ces circonstances ou de cet événement sur le cours des instruments financiers concernés ou des instruments financiers qui leur sont liés, ou encore, s'agissant plus particulièrement des catégories de quotas d'émission, sur le prix auquel les offres seraient faites sur le compartiment enchères ou sur le cours des quotas d'émission concernés ou des contrats financiers ayant pour sous-jacent un quota d'émission.

Une information susceptible d'avoir une influence sensible sur le cours des instruments financiers concernés ou le cours d'instruments financiers dérivés qui leur sont liés est une information qu'un investisseur raisonnable serait susceptible d'utiliser comme l'un des fondements de ses décisions d'investissement ou s'agissant des catégories de quotas d'émission, une information qu'un intervenant raisonnable serait susceptible d'utiliser comme l'un des fondements de ses décisions d'intervenir sur le marché.

Sont concernés les instruments financiers admis à la négociation sur un marché réglementé de l'Espace économique européen ou pour lesquels une demande d'admission a été formulée ou ceux admis sur un système multilatéral de négociation organisé.

Les opérations qui portent sur les marchés réglementés des quotas d'émission de gaz à effet de serre, celles liées à la tenue des registres ainsi que celles ayant trait aux marchés réglementés sur l'énergie et les matières premières (électricité, gaz...) sont également concernées, des règles spécifiques, notamment en ce qui concerne la définition de l'information privilégiée, pouvant trouver à s'appliquer.

Une manipulation de marché est le fait d'effectuer des opérations ou d'émettre des ordres qui :

- donnent ou sont susceptibles de donner des indications fausses ou trompeuses sur l'offre, la demande ou le cours d'instruments financiers ou qui fixent, par l'action d'une ou de plusieurs personnes agissant de manière concertée, le cours d'un ou plusieurs instruments financiers à un niveau anormal ou artificiel, à moins que la personne ayant effectué les opérations ou émis les ordres n'établisse la légitimité des raisons de ces opérations ou de ces ordres et leur conformité aux pratiques de marché admises ;
- recourent à des procédés donnant une image fictive de l'état du marché ou à toute autre forme de tromperie ou d'artifice.

CDC Informatique, GIE dont le membre principal est la Caisse des dépôts et consignations, agit dans la relation avec celle-ci comme un prestataire de services.

¹⁰ Article 7 du Règlement européen n°596/2014 du 16.04.2016 sur les abus de marché.

Application au sein de CDC Informatique

Si CDC Informatique n'est pas directement assujéti au règlement général de l'Autorité des Marchés Financiers (AMF) et aux règles strictes applicables en matière de déontologie financière, les prestations qu'il rend, concernant certaines activités, peuvent amener certains de ses collaborateurs, à l'occasion de l'exercice de leurs fonctions, à disposer d'informations confidentielles et privilégiées relatives à des émetteurs cotés.

Ainsi, il convient de rappeler et d'insister sur le fait que, dans ce cas, le droit commun s'applique et qu'ainsi **les règles qui encadrent les abus de marché** au niveau pénal (dispositions relatives aux délits d'initié, de manipulation de marché, de diffusion de fausses informations qui figurent aux articles L.465-1 et suivants du Code monétaire et Financier) et au niveau administratif (dispositions relatives aux opérations d'initiés, à la divulgation illicite d'informations privilégiées et aux manipulations de marché qui figurent dans le Règlement UE n° 596/2014 du 16 avril 2015 et dans le livre VI du règlement général de l'AMF) **sont applicables à toute personne qui a accès à certaines informations** (pas nécessairement financières) si les conditions en sont remplies.

En cas de doute, les collaborateurs peuvent demander conseil la Direction de la Maitrise des Risques, du Contrôle permanent et de la Conformité de CDC Informatique (DMRCC ICDC).

Principe 8 : Appliquer les règles relatives à l'exercice des mandats sociaux

Les collaborateurs peuvent être amenés à exercer des mandats sociaux à la demande de CDC Informatique et dans le cadre de leurs fonctions, en leur nom propre ou en tant que représentant de CDC Informatique ou du Groupe Caisse des Dépôts.

Ces mandats sont exercés dans le respect des dispositions légales et réglementaires applicables, notamment celles des articles 1984 et suivants du Code civil.

Dans ce cadre, les règles de bonne gouvernance fixées par CDC Informatique s'appliquent et encadrent, notamment, le nombre de mandats pouvant être exercés par chaque collaborateur.

Lorsque CDC Informatique envisage de confier un mandat social à l'un de ses collaborateurs, ce dernier est tenu d'attester à l'autorité hiérarchique à l'origine de la proposition son absence de conflit d'intérêts. L'autorité hiérarchique et le collaborateur s'assurent en outre du respect des règles internes en matière de cumul des mandats, en lien avec la direction des affaires juridiques, de la conformité et de la déontologie de la Caisse des Dépôts, le cas échéant.

Lorsqu'ils exercent un mandat social dans une entité du Groupe contrôlée par la Caisse des Dépôts dans le cadre de leurs fonctions, les collaborateurs veillent à la déclinaison des principes de la charte de déontologie du Groupe au sein de l'entité concernée.

Dans le cadre de ses fonctions, un mandataire social est responsable de ses actes et engage sa responsabilité civile en cas de violation de la réglementation, ou en cas de faute de gestion. Il est particulièrement vigilant au risque d'abus de bien social.

Les collaborateurs exerçant, dans le cadre de leurs fonctions au sein de CDC Informatique, des mandats sociaux tels que par exemple des fonctions d'administrateurs et/ou de membres de conseil de surveillance, en tant que représentant permanent de la Caisse des dépôts ou de l'une de ses filiales, ou en tant que personne physique, ne reçoivent ni les jetons de présence, ni les rémunérations accessoires afférentes (cf. principe 8 du Code de déontologie de la CDC).

Les informations collectées relatives aux jetons de présence et rémunérations accessoires sont enregistrées dans l'application de gestion des mandats mise à la disposition de CDC Informatique par la Caisse des dépôts, laquelle a procédé à l'enregistrement de ce traitement dans son registre des activités

de traitements de données à caractère personnel, conformément à l'article 30 du règlement général sur la protection des données (RGPD). Ce traitement vise notamment à vérifier le principe de non-perception des jetons de présence et rémunérations accessoires.

Les collaborateurs percevant des jetons de présence ou des rémunérations accessoires doivent s'engager par écrit auprès de la Direction de la Maitrise des Risques, du Contrôle permanent et de la Conformité de CDC Informatique (DMRCC) à reverser ces montants à CDC Informatique.

Principe 9 : Agir de manière loyale

Les collaborateurs qui, en sus de leurs fonctions, seraient amenés à exercer une autre activité professionnelle ou non, rémunérée ou non, s'obligent à ne pas exécuter cette autre activité si celle-ci est de nature à compromettre les intérêts de CDC Informatique, et à exécuter cette autre activité en respectant les règles déontologiques qui leur sont applicables, et ce, en vertu de leur obligation de loyauté¹¹. Cette activité secondaire doit être compatible avec les fonctions principales du collaborateur et ne pas affecter leur exercice, notamment en créant une situation de concurrence directe ou d'atteinte à la confidentialité des informations dont ils disposent.

En particulier, les collaborateurs doivent être particulièrement vigilants aux situations de conflits d'intérêts pouvant survenir.

Ils s'assurent en particulier que cette activité est compatible avec les obligations contractuelles, légales, réglementaires et conventionnelles, auxquelles ils sont soumis. Ils doivent formellement solliciter l'autorisation de la Direction des Ressources Humaines pour toute activité rémunérée exercée en dehors leur temps de travail, quelle que soit la nature de cette activité (formations, interventions à des conférences externes etc.) sauf dérogations légalement prévues (salariés à temps partiels pour la fraction du temps de travail libre, exercice d'un mandat de représentation du personnel, mandats électifs publics, etc.)¹².

La Direction des Ressources Humaines se prononce sur l'autorisation demandée par le collaborateur après avoir sollicité l'avis de La Direction de la Maitrise des Risques, du Contrôle permanent et de la Conformité de CDC Informatique (DMRCC) en matière de conflit d'intérêts. L'autorisation peut être assortie de conditions spécifiques (limitation de durée, interdiction de recours aux outils de CDC Informatique, etc.).

Pour toute modification substantielle de l'activité secondaire autorisée par la Direction des Ressources Humaines, le collaborateur est tenu de renouveler sa demande d'autorisation.

Le manquement à ces obligations peut entraîner des mesures disciplinaires à l'encontre du collaborateur.

Principe 10 : Protéger le patrimoine

Chaque collaborateur veille à un usage approprié des ressources et évite tout usage abusif, détournement ou atteinte au patrimoine matériel ou immatériel de l'entité.

Le patrimoine de CDC Informatique comprend :

- **les biens matériels** : locaux, équipements, matériels informatiques, téléphones, véhicules, fournitures, etc. ;

¹¹ L'article 1135 du Code civil dispose : « Les conventions obligent non seulement à ce qui y est exprimé, mais encore à toutes les suites que l'équité, l'usage ou la loi donnent à l'obligation d'après sa nature ». Ce principe est rappelé par l'article L. 1222-1 du Code du travail qui prévoit que le contrat de travail doit être exécuté de bonne foi. Appliqué à la relation de travail, ce principe impose au collaborateur un devoir de loyauté envers son employeur, lequel consiste à exécuter ses fonctions avec honnêteté et intégrité, et à s'abstenir de tout acte ou comportement susceptible de porter atteinte aux intérêts, au fonctionnement ou à l'image de celle-ci.

¹² Il est par ailleurs rappelé que tout cumul d'activité professionnelle avec celle exercée au bénéfice d'une entité du groupe de la Caisse des dépôts doit respecter l'article L. 8261-1 du Code du travail aux termes duquel aucun salarié ne peut accomplir des travaux rémunérés au-delà de la durée maximale du travail, telle qu'elle ressort des dispositions légales de sa profession.

- **les biens immatériels** : informations, données, logiciels, marques, savoir-faire, correspondances professionnelles, ainsi que toute contribution, conception ou résultat issus de l'activité professionnelle.

Protection du patrimoine immatériel d'ICDC

Le patrimoine immatériel est protégé par le droit de propriété intellectuelle et chaque collaborateur s'attache à respecter les droits des tiers et de CDC Informatique conformément aux dispositions du Code de la propriété intellectuelle (articles L111-1 et suivants et articles L411-1 et suivants du Code de la propriété intellectuelle).

A ce titre, les collaborateurs s'interdisent toute reproduction, utilisation ou diffusion non autorisée de logiciels, documents internes, études ou tout contenu protégé appartenant à CDC Informatique.

Utilisation des moyens matériels et numériques d'ICDC

Les installations, matériels et ressources mis à disposition par ICDC sont exclusivement utilisés pour le bon exercice des fonctions des collaborateurs et ne doivent pas être utilisés à des fins personnelles.

Toutefois, un usage ponctuel et raisonnable des ressources courantes mises à disposition par CDC Informatique à des fins personnelles est néanmoins toléré dès lors qu'il entre dans le cadre des nécessités de la vie courante et familiale, qu'il ne porte pas préjudice à CDC Informatique et qu'il est conforme à la réglementation.

Prévention des atteintes au patrimoine

Les collaborateurs sont tenus de signaler immédiatement au supérieur hiérarchique direct :

- toute perte, vol, dégradation ou incident de sécurité affectant les biens de CDC Informatique ;
- toute tentative d'intrusion, d'hameçonnage ou de détournement d'informations ;
- toute utilisation non conforme des moyens informatiques constatée.

Principe 11 : Veiller à une responsabilité sociale, sociétale et environnementale

La responsabilité sociétale et environnementale (RSE) est la manière dont CDC Informatique assume ses responsabilités et mobilise des moyens pour répondre aux enjeux sociaux, environnementaux et économiques dans ses activités.

Promouvoir l'inclusion et la diversité

Promouvoir la diversité et s'inscrire dans une démarche inclusive, c'est accorder une place à chacune et chacun, quelles que soient sa singularité, ses différences, ses opinions. C'est aussi considérer cette diversité comme créatrice de cohésion, de richesse, de bien-être, en faveur de la performance de l'entreprise.

L'ambition de CDC Informatique est de créer un impact sociétal fort, inclusif et concret. Les collaborateurs contribuent à cette démarche en veillant à :

- Adopter une attitude bienveillante dans leur comportement professionnel quotidien ;
- Favoriser l'intégration de toutes et tous dans l'environnement de travail, sans distinction ;
- Être inclusif au quotidien et dans tous les événements de la vie d'équipe (réunions, séminaires etc.).

Prévenir la discrimination

La discrimination est le traitement défavorable d'une personne physique en raison notamment de ses origines, son handicap, ses opinions, son sexe, ses orientations sexuelles, son âge, son apparence

physique, son nom, sa grosseur, ses croyances, sa situation de famille... et qui entraîne une rupture d'égalité entre les personnes notamment pour l'accès à un droit tel que l'emploi, la rémunération, l'évolution professionnelle, la protection sociale, la formation.

La loi sanctionne tout comportement qui porte atteinte à l'égalité des droits. La seule incitation ou l'instruction donnée à discriminer est également sanctionnable conformément aux articles 225-1 et suivants du Code pénal et des articles L.1132-1 et suivants du Code du travail.

CDC Informatique est engagé en faveur de la qualité de vie au travail, l'égalité des chances et de traitement et le développement professionnel.

Tous les collaborateurs sont traités avec dignité et ont les mêmes opportunités. Dans ce cadre, aucune personne au sein de l'entreprise ne peut faire l'objet d'une discrimination directe ou indirecte.

Prévenir le harcèlement et les agissements sexistes

Le harcèlement et les agissements sexistes revêtent les formes suivantes :

- Le **harcèlement moral** est le fait d'imposer à une personne, de façon répétée, des propos ou comportements ayant pour objet ou pour effet une dégradation de ses conditions de vie et/ou une altération de sa santé physique ou mentale.
- Le **harcèlement sexuel** est le fait :
 - D'imposer à une personne, de façon répétée, des propos ou comportements à connotation sexuelle ou sexiste qui, soit portent atteinte à sa dignité en raison de leur caractère dégradant ou humiliant, soit créent à son encontre une situation intimidante, hostile ou offensante ; ou
 - Lorsqu'une même personne se voit imposer de tels propos ou comportements par plusieurs personnes, de manière concertée ou à l'instigation de l'une d'elles, alors même que chacune de ces personnes n'a pas agi de façon répétée ; ou
 - Lorsqu'une même personne se voit imposer de tels propos ou comportements, successivement, venant de plusieurs personnes qui, même en l'absence de concertation, savent que ces propos ou comportements caractérisent une répétition.
- Une **pression grave dans le but d'obtenir un acte de nature sexuelle** est assimilée au harcèlement sexuel. Les faits consistent en toute forme de pression grave, même non répétée, exercée dans le but réel ou apparent d'obtenir un acte de nature sexuelle, que celui-ci soit recherché au profit de l'auteur des faits ou au profit d'un tiers.
- L'**agissement sexiste** est caractérisé par tout **agissement lié au sexe d'une personne**, ayant pour objet ou pour effet de porter atteinte à sa dignité ou de créer un environnement intimidant, hostile, dégradant, humiliant ou offensant.

Ces agissements constituent des délits passibles de sanctions pénales et disciplinaires.

Conformément à l'article L. 4121-1 du Code du travail, CDC Informatique s'engage à maintenir un environnement de travail qui protège les collaborateurs dans toutes les situations de travail, contre toute forme de harcèlement et d'agissements sexistes par la mise en place d'un dispositif de prévention, d'alerte et d'accompagnement disponible sur l'intranet.

Garantir la santé, la sécurité et la qualité de vie au travail

CDC Informatique a l'obligation légale et morale d'assurer **la santé et la sécurité de ses collaborateurs** ainsi que de l'ensemble des personnes qui fréquentent ses établissements. La santé et la sécurité au travail recouvrent notamment la prévention des accidents du travail ou de trajet, des maladies professionnelles et des risques psychosociaux.

CDC Informatique met en œuvre une démarche de prévention. Il coordonne les différentes équipes et attribue les moyens nécessaires à la préservation de la santé physique et mentale de ses collaborateurs ainsi que de toutes personnes travaillant pour son compte présentes dans ses locaux.

Un document unique d'évaluation des risques professionnels (DUERP) est tenu à jour conformément à l'article R.4121-1 du Code du travail.

En signant des accords sur la qualité de vie au travail, CDC Informatique inscrit cet enjeu au cœur de ses objectifs stratégiques en faveur des salariés de l'entreprise et veille également à l'équilibre entre vie privée et vie professionnelle.

Protéger l'environnement

Chaque Collaborateur veille au respect de l'environnement.

CDC Informatique, à l'instar du Groupe Caisse des dépôts, a pour objectif d'atteindre les meilleurs standards en matière de protection de l'environnement.

Fort de cet engagement, CDC Informatique s'efforce de minimiser son empreinte écologique. CDC Informatique est Labelisé Numérique Responsable (NR). Soucieux de son impact environnemental, CDC Informatique intègre le NR dans ses pratiques, notamment l'éco-conception et l'accessibilité qui sont au cœur de ses projets.

Par ailleurs, CDC Informatique a mis en place un schéma de promotion des achats socialement et écologiquement responsables (SPASER) permettant à CDC Informatique de définir une stratégie d'achats durables.

Il appartient à chaque collaborateur, dans la limite de ses fonctions, de contribuer aux efforts et aux engagements de CDC Informatique en matière de responsabilité sociale et environnementale.

Principe 12 : Mettre en place un dispositif d'alerte professionnelle

En application du chapitre II de la loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique (dite « loi Sapin 2 ») et de la loi 2022-401 du 21 mars 2022 (dite loi Wasserman) et de son décret d'application n°2022-1284 du 3 octobre 2022, CDC Informatique met à la disposition de ses collaborateurs un dispositif approprié de recueil des signalements conforme au « référentiel relatif aux traitements de données à caractère personnel destinés à la mise en œuvre d'un dispositif d'alerte » en date du 6 juillet 2023 de la Commission Nationale de l'Informatique et des Libertés (ci-après la « CNIL ») qui actualise le référentiel initialement publié en 2019 (ci-après le « Référentiel »).

Ce dispositif de recueil des signalements est mis en place par CDC Informatique conformément à sa culture, sa taille et sa structure et tient compte des différents risques et enjeux que la mise en œuvre d'un tel dispositif peut présenter.

Conformément à l'article 8 de la loi Sapin II, le lanceur d'alerte peut être toute personne physique telle que :

- les membres du personnel¹³, les personnes dont la relation de travail s'est terminée, lorsque les informations ont été obtenues dans le cadre de cette relation, et les personnes qui se sont portées candidates à un emploi au sein de CDC Informatique, lorsque les informations ont été obtenues dans le cadre de cette candidature ;
- les titulaires de droits de vote au sein de l'assemblée générale de CDC Informatique ;

¹³ Les membres du personnel sont ci-après désignés sous le terme « collaborateurs », dans la présente procédure, et couvrent tous salariés de CDC Informatique, y compris les alternants.

- les membres de l'organe d'administration, de direction ou de surveillance ;
- les collaborateurs extérieurs et occasionnels¹⁴ ;
- les cocontractants de CDC Informatique¹⁵, leurs sous-traitants ou, lorsqu'il s'agit de personnes morales, les membres de l'organe d'administration, de direction ou de surveillance de ces cocontractants et sous-traitants ainsi que les membres de leur personnel.

Conformément à l'article 6 de la loi n° 2016-1691 du 9 décembre 2016, le dispositif d'alerte mis en place au sein de CDC Informatique peut être utilisé pour signaler, sans contrepartie financière directe et de bonne foi, à la Déontologue désignée par CDC Informatique, des informations portant sur :

- un crime ou un délit (*tels que corruption, trafic d'influence, autre manquement à la probité, blanchiment d'argent, fraude, escroquerie, abus de biens sociaux, détournement d'actifs et vol*) ;
- une menace ou un préjudice pour l'intérêt général (*tels que des agissements susceptibles de faire courir un danger ou une atteinte à la sécurité de la population dans le domaine de la santé ou de l'environnement*) ;
- 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 ou du droit de l'Union européenne (*telle qu'une atteinte aux droits de l'homme et aux libertés fondamentales*) ;
- une violation ou une tentative de dissimulation d'une violation de la loi ou du règlement.

Lorsque les informations n'ont pas été obtenues dans le cadre de ses activités professionnelles, le lanceur d'alerte doit en avoir eu personnellement connaissance.

Ce dispositif d'alerte est un outil d'utilité sociale et économique à la disposition de chacun des collaborateurs de CDC Informatique. L'utilisation de ce dispositif est facultative, de sorte qu'aucun collaborateur ne pourra se voir sanctionné, de quelque manière que ce soit, pour ne pas l'avoir utilisé.

Grâce à ce dispositif, chacun devient un acteur de la démarche commune de prévention des risques et de déontologie mise en œuvre par CDC Informatique.

Les personnes pouvant émettre une alerte (telles que définies ci-dessus par l'article 8 de la loi Sapin II) peuvent adresser leur signalement par écrit par l'un quelconque des moyens suivants :

- par courrier électronique à l'adresse dédiée suivante : deontologie-icdc@caissedesdepots.fr ;
- par courrier recommandé avec demande d'avis de réception à l'adresse suivante : CDC Informatique, à l'attention de la Déontologue de CDC Informatique (DMRCC) 18 avenue Aristide Briand, 92220 Bagneux.

Il est recommandé que l'envoi postal soit effectué sous double enveloppe : une enveloppe intérieure comprenant les éléments de l'alerte, sur laquelle figure la mention « signalement d'une alerte », la mention « confidentiel » et la date de l'alerte et une enveloppe extérieure adressée au déontologue.

Le traitement de ces signalements est conduit avec diligence par la Déontologue, dans le respect de la réglementation en vigueur et dans la plus stricte confidentialité et impartialité, en garantissant la protection du lanceur d'alerte. Les conditions d'exercice de ce droit d'alerte et les modalités de leur traitement sont précisées dans la procédure d'alerte professionnelle disponible sur le site internet de CDC Informatique ainsi que sur l'intranet de CDC Informatique.

¹⁴ Il s'agit notamment des intérimaires ou encore des stagiaires.

¹⁵ Il s'agit notamment des prestataires de service ayant un contrat en cours avec CDC Informatique ainsi que leurs salariés, des fournisseurs de CDC Informatique, des partenaires liés par un contrat, etc.

La « Fonction déontologie » et son organisation au sein de CDC Informatique

Fonctions de la DAJCD CDC/service déontologie de la CDC et de la filière déontologie

A titre liminaire, d'une manière générale, la fonction Déontologie est organisée dans le groupe CDC sous la forme d'une filière dont l'objectif est d'assurer la cohérence de l'ensemble des règles prescrites au sein de l'Etablissement public et des filiales.

La Direction des Affaires Juridiques, Conformité et Déontologie (DAJCD) anime le dispositif déontologique du Groupe et est directement chargée de la déontologie propre à l'Etablissement public. Pour l'ensemble du Groupe, elle anime un réseau de correspondants comprenant les correspondants au sein des directions de la Caisse des dépôts et les déontologues des filiales.

Les déontologues des filiales sous contrôle exclusif¹⁶ adoptent le Code de déontologie du Groupe CDC dans sa totalité ou en transposent les principes en expliquant auprès de DAJCD les éventuelles modifications qui s'avèreraient nécessaires au vu de la nature de l'activité.

CDC Informatique a transposé les principes fondamentaux du Code de déontologie de Groupe en les adaptant à son activité.

Fonctions et organisation de DMRCC en matière de déontologie

Le service Déontologie de DMRCC s'assure du respect des règles de déontologie du présent Code.

A ce titre, il veille à ce que les Directions de CDC Informatique mettent en œuvre les moyens adaptés pour satisfaire aux dispositions qui leur sont applicables, et réalise des contrôles de niveau 1.

Le service Déontologie s'assure que le Code de déontologie ICDC est toujours conforme au Code de déontologie du Groupe CDC.

La (le) Déontologue de CDC Informatique rend compte de sa mission au Directeur Général de CDC Informatique et peut être contrôlée par DAJCD ou DRG (Direction des Risques Groupe).

Diffusion des normes de déontologie

Le Code de déontologie de CDC Informatique est mis à disposition des collaborateurs sur l'intranet de CDC Informatique à la rubrique déontologie et remis aux nouveaux arrivants par la Direction des Ressources Humaines. Le code de déontologie de CDC Informatique est également publié sur son site internet <https://www.icdc.caissedesdepots.fr/>.

Formation et conseil aux collaborateurs

• Formation des collaborateurs

Les collaborateurs doivent suivre tous les deux ans une formation en matière de déontologie.

¹⁶ Les filiales dites sous contrôle exclusif s'entendent des entités de toute nature (y compris les GIE) dans lesquelles la Caisse des dépôts :

- détient, directement ou indirectement, un pourcentage de contrôle supérieur à 50 %, c'est à dire la majorité des droits de vote (contrôle de droit),
- est actionnaire de l'entreprise et y exerce une influence dominante en vertu d'un contrat ou de clauses statutaires (contrôle contractuel),
- désigne, pendant deux exercices, la majorité des membres de direction et d'administration (contrôle de fait démontré),
- dispose, pendant deux ans, d'une fraction supérieure à 40% des droits de vote et si aucun autre associé ne détient une part supérieure (contrôle de fait présumé).

- **Conseil aux collaborateurs**

Le service Déontologie conseille les collaborateurs ou formule des avis sur la conduite à tenir lorsqu'une question ou un doute apparaît par rapport à une situation.

En cas d'interrogation concernant une situation particulière ou sur l'interprétation du Code de déontologie, le service Déontologie peut être contactée via l'adresse courriel suivante : deontologie-icdc@caissedesdepots.fr.

Comité de déontologie ICDC

Le comité déontologie se tient lors des comités risques ICDC (CRCI) qui ont lieu semestriellement, ou dès qu'un cas nécessite sa saisine (Cf. Charte de gestion des risques, de contrôle permanent et de la conformité).

Relation avec les autorités de supervision

L'obligation de confidentialité n'est pas opposable lorsqu'il s'agit de communiquer les informations requises par la loi ou les règlements.

En outre, le secret professionnel ne doit pas faire obstacle aux déclarations obligatoires imposées par la législation relative à la lutte contre le blanchiment et le financement du terrorisme et aux abus de marché.

Afin de répondre aux questions posées dans le cadre des contrôles sur place ou sur pièce, la Direction Générale de CDC Informatique est l'interlocutrice de l'Autorité de Contrôle Prudentiel et de Résolution (ACPR). La Direction Générale délègue à la DMRCC ICDC cette faculté.

Tout collaborateur directement contacté par l'ACPR doit immédiatement prévenir son responsable hiérarchique qui en informera la DMRCC ICDC.

Contrôle

Les collaborateurs et leur hiérarchie coopèrent avec les organes de contrôle et d'audit, internes et externes, et remédient avec promptitude aux défauts et aux dysfonctionnements constatés.

Déclaration d'incidents

Les incidents de déontologie étant considérés comme des incidents significatifs par nature, ils sont déclarés par les métiers concernés dans la base incidents (PRISM) administrée par DRG.

Versions	Nature des modifications	Entrée en vigueur
V1	<ul style="list-style-type: none"> Réunion de toutes les règles déontologiques existantes à ICDC en un Code de déontologie avec ajout du dispositif d'alerte professionnelle (Loi Sapin II du 9 décembre 2016). 	01 04 2018
V2	<ul style="list-style-type: none"> Référence au décret du 5 février 2020 relatif aux règles de contrôle interne applicables à la Caisse des dépôts Mise en conformité avec les règles du groupe Caisse des dépôts : lutte contre la corruption, lutte contre la fraude, politique relative aux conflits d'intérêts, protection du patrimoine ; Mise en conformité avec le RGPD (notamment les règles de conservation des données à caractère personnel). 	01 01 2022
V3	<ul style="list-style-type: none"> Modification du nom de la directrice des risques et déontologue ; Mise en conformité avec la loi dite Wasserman du 21 mars 2022 pour une protection accrue du lanceur d'alerte ; Ajout du principe de tolérance zéro face à la corruption, au trafic d'influence et à l'ensemble des manquements à la probité, et ce, en conformité avec les préconisations de DCPC (novembre 2022). 	01 09 2023
V4	<ul style="list-style-type: none"> Mise à jour de l'adresse d'ICDC à la suite au changement de siège social résultant du déménagement à Bagneux en juillet 2024 ; Remplacement de Informatique CDC par CDC Informatique suite au changement de dénomination sociale Remplacement du nom DRCI par DMRCC (Direction de la Maîtrise des Risques, du Contrôle et de la Conformité) ; Transposition au sein du Code de déontologie de CDC Informatique de certaines dispositions du Code de déontologie de la Caisse des dépôts mis à jour en janvier 2025 Extraction et modification de l'Annexe 1 « Procédure Cadeaux et Avantages » pour en faire une procédure à part entière et distincte ; Extraction et modification de l'Annexe 2 « Procédure de gestion des Conflits d'intérêts » pour en faire une procédure à part entière et distincte ; Extraction et modification de l'Annexe 3 « Alerte professionnelle » pour en faire une procédure à part entière et distincte Ajout du principe « Veiller à une responsabilité sociale, sociétale et l'environnementale » Création d'une fiche réflexe 	Sept 2025

CE QU'IL FAUT RETENIR

Tous ensemble, respectons nos valeurs

Le Code de déontologie de CDC Informatique nous engage tous à porter les valeurs de CDC Informatique, à les respecter, et à les faire respecter dans nos actes quotidiens.

LES RÉFLEXES ESSENTIELS QUE VOUS DEVEZ AVOIR POUR ADOPTER UNE CONDUITE ÉTHIQUE



AVANT D'AGIR

Se poser les bonnes questions :

- Votre décision ou votre action est-elle conforme à la loi ?
- Votre décision ou votre action est-elle conforme au **Code de déontologie de CDC Informatique et aux Chartes, politiques, et procédures** de CDC Informatique ?
- Votre décision ou votre action **est-elle guidée** par votre intérêt personnel ou celui de vos proches ?
- Votre décision ou votre action peut-elle avoir un **impact négatif** sur CDC Informatique, sur le groupe Caisse des Dépôts, sur vos collègues ou sur les parties prenantes avec lesquelles vous interagissez ?

Consulter les Chartes, politiques et procédures mises à votre disposition par CDC Informatique pour **vous protéger et vous aider dans vos choix**. Elles approfondissent les différents sujets abordés dans le Code de conduite.



DEMANDER CONSEIL

Tout collaborateur confronté à une situation évoquée dans le présent Code de déontologie peut se rapprocher de son manager, de la DRH et/ou du service Déontologie de DMRCC ICDC pour connaître la conduite à tenir.



ALERTER

- Signalez tout manquement au présent Code de déontologie auprès de votre hiérarchie et/ou au service Déontologie.
