## INTRODUCTION – *INTRODUCTION – INTRODUCCIÓN – EINLEITUNG – INTRODUCTIE – INTRODUZIONE*

Le groupe Circet est attaché au respect d'un ensemble de valeurs, principes, normes, règles, standards et directives, visant à un comportement respectueux envers les personnes et l'environnement et permettant une conduite éthique des affaires, rappelés notamment dans son **Code de conduite anticorruption**.

***English -*** *The Circet group is committed to a set of values, principles, norms, rules, standards, and directives aimed at ensuring a responsible behavior towards people and the environment and driving our business ethically, reminded notably in the Code of conduct preventing bribery.*

***Spanish -*** *El grupo Circet se ha comprometido a respetar un conjunto de valores, principios, normas, reglas, estándares y directrices, dirigidos a un comportamiento respetuoso con las personas y el entorno y a permitir una conducta comercial ética, como se recuerda en particular en su Código de Conducta Anticorrupción.*

***German*** *- Die Circet-Gruppe verpflichtet sich zur Einhaltung einer Reihe von Werten, Grundsätzen, Normen, Regeln, Standards und Richtlinien, die auf ein respektvolles Verhalten gegenüber Mensch und Umwelt abzielen und ein ethisches Geschäftsgebaren ermöglichen, worauf insbesondere in ihrem Verhaltenskodex zur Korruptionsbekämpfung hingewiesen wird.*

***Nederlands*** *- De Circet Groep verplicht zich tot het naleven van een reeks waarden, principes, normen, regels, standaarden en richtlijnen die erop gericht zijn om respectvol om te gaan met mens en milieu en ethische handelspraktijken te hanteren. Met name de gedragscode tegen corruptie herinnert hieraan.*

***Italian*** *- Il Gruppo Circet è impegnato in un insieme di valori, principi, norme, regole, standard e linee guida, che mirano ad un comportamento rispettoso nei confronti delle persone e dell'ambiente e che permettono una condotta etica degli affari, fatti presente in particolare nel suo Codice di condotta anticorruzione.*

Tout employé ou agent ou partenaire commercial agissant en au nom et pour le compte du groupe est encouragé à signaler des faits dont il a eu personnellement connaissance concernant un problème de corruption, trafic d'influence ou actes similaires le plus tôt possible à son responsable hiérarchique ou au responsable du chantier/du contrat (pour un collaborateur externe).

***English*** *- Each employees or any agent or commercial partner acting in the name of and on the behalf of the group is encouraged to report facts of which they became personally aware of in respect of cases of bribery, influence peddling, or similar actions to their line manager or the manager of the site/contract (for an external collaborator) as soon as possible.*

***Spanish -*** *Se alienta a todo empleado o agente o socio comercial que actúe en nombre y representación del Grupo que comunique lo antes posible a su superior o a la persona encargada del lugar de trabajo/contrato (en el caso de un colaborador externo) los hechos personalmente conocidos en relación con un problema de corrupción, tráfico de influencias o actos similares.*

***German*** *- Jeder Mitarbeiter, Vertreter oder Geschäftspartner, der im Namen und im Auftrag der Gruppe handelt, wird ermutigt, Tatsachen, von denen er persönlich Kenntnis hat und die ein Problem der Bestechung, des Handels mit Einfluss oder ähnlicher Handlungen betreffen, so schnell wie möglich seinem Vorgesetzten oder der für die Baustelle/den Vertrag verantwortlichen Person (im Falle eines externen Mitarbeiters) zu melden.*

***Nederlands*** *- Elke werknemer, agent of zakenpartner die in naam en voor rekening van de Groep handelt, wordt aangemoedigd om feiten waarvan hij of zij persoonlijk kennis heeft met betrekking tot een probleem van omkoping, beïnvloedingspraktijken of soortgelijke handelingen zo snel mogelijk te melden aan zijn of haar lijnmanager of aan de persoon die verantwoordelijk is voor de bouwplaats/het contract (in het geval van een externe medewerker).*

***Italian*** *- Ogni dipendente o agente o partner commerciale che agisce per conto del Gruppo è incoraggiato a riferire fatti di cui è personalmente a conoscenza in materia di corruzione, commercio di influenza o atti simili il più presto possibile al suo manager di linea o alla persona responsabile del sito/contratto (nel caso di un dipendente esterno).*

En complément des canaux traditionnels et conformément à la loi française 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 « Sapin II » et selon les modalités énoncées par le décret français n° 2017-564 du 19 avril 2017, un dispositif de recueil des signalements a été mis en place.

***English*** *- In addition to the traditional channels and in accordance with French law no. 2016-1691 of 9 December 2016 on transparency, the fight against corruption and the modernisation of economic life, known as "Sapin II", and in accordance with the procedures set out in French decree no. 2017-564 of 19 April 2017, a whistleblowing tool has been set up.*

***Spanish*** *- Además de los canales tradicionales y de conformidad con la Ley francesa Nº 2016-1691, de 9 de diciembre de 2016, relativa a la transparencia, la lucha contra la corrupción y la modernización de la vida económica, conocida como "Sapin II", y con arreglo a los procedimientos establecidos en el Decreto francés Nº 2017-564, de 19 de abril de 2017, se ha establecido un sistema de recogida de alertas.*

***German*** *- Zusätzlich zu den traditionellen Kanälen und gemäß dem französischen Gesetz Nr. 2016-1691 vom 9. Dezember 2016 über Transparenz, Korruptionsbekämpfung und Modernisierung des Wirtschaftslebens, bekannt als "Sapin II", und den im französischen Erlass Nr. 2017-564 vom 19. April 2017 festgelegten Richtlinien, wurde ein System zur Sammlung von Warnmeldungen eingerichtet.*

***Nederlands*** *- Naast de traditionele kanalen en overeenkomstig de Franse wet nr. 2016-1691 van 9 december 2016 betreffende transparantie, corruptiebestrijding en de modernisering van het economische leven, bekend onder de naam "Sapin II", en overeenkomstig de procedures die zijn vastgesteld in het Franse decreet nr. 2017-564 van 19 april 2017, werd er een meldingssysteem opgezet.*

***Italian*** *- Oltre ai canali tradizionali e conformemente alla legge francese n. 2016-1691 del 9 dicembre 2016 sulla trasparenza, la lotta contro la corruzione e la modernizzazione della vita economica, detta*

*"Sapin II", e secondo le modalità previste dal decreto francese n. 2017-564 del 19 aprile 2017, è stato messo in atto un sistema di raccolta delle segnalazioni.*

La procédure qui suit a pour objet de déterminer les modalités de recueil des signalements. Les filiales du groupe implantées dans un pays autre que la France, déterminent si, compte-tenu de leur législation nationale, la présente procédure peut être appliquée telle quelle.

***English*** *- The following procedure is intended to determine how alerts are to be collected. The subsidiaries of the group established in a country other than France shall determine whether, in view of their national legislation, this procedure can be applied as it stands.*

***Spanish*** *El siguiente procedimiento trate de determinar cómo se recogen las alertas. Las filiales del grupo establecidas en un país distinto de Francia determinarán si, a la luz de su legislación nacional, este procedimiento puede aplicarse tal como está.*

***German*** *Das folgende Verfahren soll bestimmen, wie die Hinweise gesammelt werden. Die Tochtergesellschaften der Gruppe, die in einem anderen Land als Frankreich niedergelassen sind, entscheiden, ob dieses Verfahren im Lichte ihrer nationalen Gesetzgebung in der vorliegenden Form angewendet werden kann.*

***Nederlands*** *- De volgende procedure is bedoeld om te bepalen hoe waarschuwingen worden verzameld. De dochterondernemingen van de groep die in een ander land dan Frankrijk zijn gevestigd, bepalen of deze procedure in het licht van hun nationale wetgeving in haar huidige vorm kan worden toegepast.*

***Italian*** *- Lo scopo della seguente procedura è di determinare come vengono raccolti le segnalazioni. Le filiali del gruppo situate in un paese diverso dalla Francia determinano se, alla luce della loro legislazione nazionale, questa procedura può essere applicatanella sua forma attuale.*

# SOMMAIRE – *SUMMARY- SUMARIO – INHALTVERZEICHNIS – INHOUDSOPGAVE – SOMMARIO*

# 1. PROCEDURE RELATIVE AUX LANCEURS D'ALERTES

## 1. RESUME

Les salariés et collaborateurs externes ou occasionnels du Groupe CIRCET (« l'organisation ») peuvent porter à son attention, de manière confidentielle, toute atteinte grave à l'intérêt général et aux dispositions de son code de conduite. Le bon fonctionnement de l'organisation amène à ce que ceux-ci puissent informer l'organisation d'un manquement possible ou avéré aux dispositions légales et réglementaires, ainsi qu'aux procédures internes.

La procédure décrite ci-après (la « Procédure ») permet à ceux qui le souhaitent d'exercer leur droit d'alerte et de bénéficier de la protection des lanceurs d'alerte prévue par 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 et selon les modalités énoncées par le décret n° 2017-564 du 19 avril 2017.

Cette Procédure est facultative et l'organisation ne prendra aucune mesure à l'encontre de ceux qui ne l'utiliseraient pas. Elle n'a pas pour objet de se substituer aux voies normales de communication interne qui se font au travers de la structure hiérarchique de l'organisation et auprès du supérieur hiérarchique direct ou indirect, la direction des Ressources Humaines, ou encore un représentant des salariés ou du personnel : elle a donc un caractère subsidiaire.

Des précautions particulières sont prévues par l'organisation pour encadrer le traitement de ces alertes, conformément aux lois et réglementations applicables, en ce compris la délibération n° 2017-191 du 22 juin 2017 portant modification de la délibération n° 2005-305 du 8 décembre 2005 portant autorisation unique de traitements automatisés de données à caractère personnel mis en œuvre dans le cadre de dispositifs d'alerte professionnelle (AU-004) de la CNIL (Commission Nationale Informatique et Liberté) et suite à l'analyse d'impact relative à la protection des données (AIPD) effectuée par l'organisation en application de la délibération n° 2018-327 de la CNIL.

## 2. LE DROIT D'ALERTE

2.1. Le droit d'alerte peut se résumer en la faculté offerte à toute personne de décider ou non de signaler une atteinte grave à l'intérêt général dont il a personnellement connaissance.

2.2. L'alerte peut avoir pour objet tout crime ou délit, toute violation grave et manifeste d'un règlement, d'une loi ou d'un traité international ratifié par la France, ou enfin toute menace ou préjudice grave pour l'intérêt général[1].

2.3. Par exemple, l'alerte peut porter sur tout fait ou comportement constitutif d'une violation des règles en matière de lois et règlements.

[1] Les faits, informations ou documents, quels que soit leur forme ou leur support, couverts par le secret de la défense nationale, le secret médical ou le secret des relations entre un avocat et son client sont exclus du régime de l'alerte défini par cette Procédure.

2.4. Toute situation qui ne parait pas conforme aux dispositions du code de conduite de l'organisation peut également faire l'objet d'un signalement.

## 3. LE LANCEUR D'ALERTE

3.1. Tous les collaborateurs internes (salariés à temps plein, partiel, temporaire, apprentis et stagiaires) et collaborateurs externes ou occasionnels (y compris les sous-traitants ou fournisseurs) de l'organisation peuvent signaler une alerte. Les personnes prenant part à des activités en lien avec l'organisation mais sans que l'organisation les organise, sont invitées à signaler leur alerte auprès de l'organisme organisateur de l'activité.

3.2. Pour lancer une alerte il faut nécessairement être :
(a) une personne physique,
(b) agissant de bonne foi,
(c) de manière désintéressée,
(d) signalant des faits dont il a eu personnellement connaissance et
(e) en respectant la Procédure telle que détaillée en Section 4.

3.2.1. Le signalement doit être fait de bonne foi, c'est-à-dire en ayant la croyance raisonnable que les faits sont vrais au moment de leur signalement.

3.2.2. Le signalement doit être désintéressé, c'est à dire que son auteur ne prétend pas à une rémunération, à un avantage ou à une contrepartie, et n'agit pas avec l'intention de nuire à autrui.

3.2.3. Enfin, le lanceur d'alerte doit avoir eu personnellement connaissance des faits qu'il rapporte. Le signalement de faits dont on n'a pas eu personnellement connaissance, qui ont été rapportés par une autre personne, ou qui relèvent du soupçon ou de l'allégation non étayée, sera considéré comme irrecevable.

## 4. SIGNALER UNE ALERTE

4.1. Les collaborateurs internes de l'organisation peuvent effectuer un signalement directement auprès des référents spécialement désignés par l'organisation pour recevoir et analyser les alertes (les **«** Référent Alertes **»**) ainsi que via notre plateforme de signalement accessible en ligne.

Il est rappelé que ce procédé est subsidiaire et ne se substitue pas aux voies normales de communication interne qui se font au travers de la structure hiérarchique de l'organisation, tel le supérieur hiérarchique direct ou indirect, la direction des Ressources Humaines, ou encore un représentant des salariés ou du personnel, que les collaborateurs internes sont invités à utiliser.

4.2. Les collaborateurs externes à l'organisation peuvent effectuer un signalement auprès du Référent Alertes, ainsi que via notre plateforme de signalement accessible en ligne.

4.3. Le signalement doit comporter tout élément de fait, informations ou documents pertinents permettant d'étayer l'alerte, afin que le signalement soit aussi exhaustif, précis, circonstancié et documenté que possible ; en particulier, le signalement devra préciser la date à laquelle les faits se sont déroulés et l'identité des personnes impliquées lorsque ces éléments sont connus de l'auteur de l'alerte.

4.4. L'auteur précise les raisons de sa connaissance personnelle des faits, et si un tiers a été informé, par l'auteur de l'alerte ou par un autre moyen, des mêmes faits.

4.5. L'auteur de l'alerte est invité à fournir tout élément d'information qui permettront à l'organisation, tout en préservant la confidentialité de son identité, de le contacter (nom, prénoms, modalités de contact) et d'échanger sur l'alerte.

4.6. Par exception, une alerte anonyme pourra être traitée à condition que la gravité des faits mentionnés soit établie et que les éléments factuels soient suffisamment détaillés. Le traitement de cette alerte sera entouré de précautions spécifiques, telles qu'un examen préalable par son premier destinataire, ou encore de l'opportunité de sa diffusion dans le cadre du dispositif. Le site internet sécurisé de la plateforme dédiée permet l'anonymat mais ne l'encourage pas. Il est plus difficile et même parfois impossible de traiter un signalement anonyme ou d'établir que les faits sont fondés. L'organisation recommande que l'alerte soit nominative ; le processus d'enquête est en effet facilité lorsque l'identité de son auteur est connue afin de pouvoir échanger avec lui, étant noté que l'organisation s'engage à en préserver la confidentialité.

## 5. CONFIDENTIALITE

5.1. L'organisation garantit la stricte confidentialité de :
- 5.1.1. L'identité de l'auteur d'une alerte,
- 5.1.2. L'identité des personnes visées par l'alerte,
- 5.1.3. De toutes les informations recueillies dans le cadre du traitement de l'alerte.

5.2. Une fois le signalement recueilli, l'échange entre le Référent Alertes (et/ou ses délégués éventuels) et l'auteur du signalement se fait via la plateforme de signalement. L'absence de recours à cette messagerie, ou l'utilisation d'autres moyens de communication, n'affecte pas l'éventuelle recevabilité de l'alerte, ni n'expose son auteur à des sanctions. L'accès à la messagerie de la plateforme est réservé aux Référent Alertes et à ses délégués éventuels.

5.3. En cas de signalement d'alerte par courrier, il est recommandé d'utiliser la méthode de Double-enveloppe : tous les éléments de l'alerte sont insérés dans une enveloppe fermée - dite enveloppe intérieure - qui sera elle-même insérée dans une seconde enveloppe.

## 6. TRAITEMENT DES ALERTES

6.1. La vérification, le traitement et l'analyse des alertes sont effectués par l'organisation dans les meilleurs délais et dans le respect du caractère confidentiel de l'alerte. L'auteur de l'alerte n'est pas invité à conduire sa propre enquête, ni à chercher à établir la qualification juridique des faits rapportés.

6.2. L'auteur de l'alerte recevra immédiatement via la plateforme une confirmation de transmission de son signalement et devra conserver son code confidentiel. La confirmation de bonne transmission ne vaut pas recevabilité du signalement.

6.3. L'examen de la recevabilité de l'alerte s'effectue dans un délai raisonnable n'excédant pas en principe 15 jours ouvrés, après réception de l'alerte. L'auteur est tenu informé de sa recevabilité. Si le signalement est recevable, une enquête sera effectuée afin de déterminer la réalité des faits rapportés.
- 6.3.1. Les délais peuvent néanmoins varier en fonction des éléments de l'alerte.

6.4. Si, à l'issue d'un délai raisonnable après avoir signalé une alerte, son auteur n'a pas été tenu informé de sa recevabilité, il pourra adresser son signalement aux autorités judiciaires (par exemple : procureur, juge) ou administratives (par exemple : préfet; Commission Nationale de l'Informatique et des Libertés–CNIL; Agence Française Anticorruption–AFA). En dernier ressort et à défaut de traitement par l'une de ces autorités dans un délai de trois mois, l'auteur de l'alerte pourra la rendre publique (par exemple : signalement aux medias, à une association, à une ONG ou à un syndicat).

6.5. L'alerte ne peut être directement portée à la connaissance des autorités compétentes ou être rendue publique qu'en cas de danger grave et imminent, ou en présence d'un risque de dommage irréversible.

6.5.1. On entend par danger grave et imminent tout type de danger susceptible d'entrainer des blessures ou la mort, et dont la réalisation est proche.

6.6. En cas de doute, toute personne peut adresser son signalement au Défenseur des droits afin d'être orientée vers l'organisme approprié de recueil de l'alerte. Le signalement d'une alerte au Défenseur des droits devra lui être adressé par la poste par écrit sous double-enveloppe. Tous les éléments de la saisine doivent être insérés dans une enveloppe fermée – dite enveloppe intérieure – qui sera insérée dans une seconde enveloppe adressée au Défenseur des droits, dite enveloppe extérieure. Sur l'enveloppe intérieure figurera exclusivement la mention suivante : **«** SIGNALEMENT D'UNE ALERTE AU TITRE DE LA LOI DU 9 DECEMBRE 2016 EFFECTUE LE (date de l'envoi). **»** Sur l'enveloppe extérieure figurera l'adresse : Défenseur des droits, Libre réponse 71120, 75342 PARIS CEDEX 07**.**

## 7. PROTECTION CONTRE LES REPRESAILLES

7.1. L'organisation protège tout individu ayant, de manière désintéressée et de bonne foi, porté à son attention des faits constitutifs d'un délit ou d'un crime, même si les faits signalés devaient se révéler inexacts, ou ne devaient donner lieu à aucune suite.

7.2. Aucun individu ne pourra être écarté d'une procédure de recrutement ou de l'accès à un stage ou à une période de formation, et aucun salarié ne pourra être sanctionné, licencié ou faire l'objet d'une mesure discriminatoire, directe ou indirecte, notamment en matière de rémunération, de mesures d'intéressement ou de distribution d'actions, de formation, de reclassement, d'affectation, de qualification, de classification, de promotion professionnelle, de mutation ou de renouvellement de contrat.

7.3. Tout salarié ou collaborateur estimant avoir fait l'objet de représailles pour avoir relaté ou témoigné, de bonne foi, des faits constitutifs d'un délit ou d'un crime dont il aurait eu connaissance dans l'exercice de ses fonctions, pourra le signaler au Référent Alertes, ou saisir le tribunal des prud'hommes en référé en cas de licenciement.

7.4. Tout utilisation abusive du dispositif, sous la forme notamment de signalement calomnieux (signalement d'informations que l'on sait totalement ou partiellement inexactes) ou effectué de mauvaise foi expose son auteur aux poursuites prévues par la loi (article 226-10 du code pénal) et, conformément au Règlement Intérieur, à des sanctions disciplinaires.

7.5. Tout salarié faisant ou ayant fait obstacle à la transmission d'une alerte, ou ayant pris des mesures de représailles à l'encontre de l'auteur d'un signalement s'expose à des poursuites judiciaires et pourra, conformément au Règlement Intérieur, faire l'objet de sanctions disciplinaires.

## 8. TRAITEMENT DES DONNEES PERSONNELLES

8.1. L'organisation n'enregistre, dans le cadre du traitement d'une l'alerte, que les données suivantes :

- 8.1.1. identité, fonctions et coordonnées de l'auteur du signalement ;
- 8.1.2. identité, fonctions et coordonnées des personnes faisant l'objet d'une alerte ;
- 8.1.3. identité, fonctions et coordonnées des personnes intervenant dans le recueil ou dans le traitement de l'alerte ;
- 8.1.4. faits signalés ;
- 8.1.5. éléments recueillis dans le cadre de la vérification des faits signalés ;
- 8.1.6. compte rendu des opérations de vérification ;
- 8.1.7. suites données à l'alerte.

La collecte et le traitement de ces données personnelles ont pour but de déterminer l'admissibilité des signalements, de vérifier les faits et de prendre les mesures correctives s'imposant le cas échéant. Ils permettent ainsi à l'organisation de respecter ses obligations légales (issues en particulier de la loi dite "Sapin 2" du 9 décembre 2016 et de la loi du 27 mars 2017 relative au devoir de vigilance) et de protéger ses intérêts légitimes (par le respect de la loi et des principes éthiques de l'organisation).

8.2. Le droit d'accès, de rectification et d'opposition à l'utilisation des données peut être exercé, dans le cadre légal et réglementaire, en contactant le Référant Aux Alertes à l'adresse.

8.3. En aucun cas, la personne qui fait l'objet d'une alerte ne peut obtenir communication de la part du responsable du traitement, des informations concernant l'identité de l'auteur de l'alerte.

8.4. L'émetteur de l'alerte ou la personne faisant l'objet d'une alerte peuvent se faire assister par toute personne de leur choix appartenant à l'organisation et ce, à tous les stades du dispositif.

8.5. Toute donnée relative à une alerte qui serait considérée comme n'entrant pas dans le champ du dispositif de la présente procédure sera supprimée ou archivée après anonymisation par l'organisation.

8.6. Si aucune suite n'est donnée à une alerte, l'organisation détruira tous les éléments du dossier d'alerte permettant d'identifier son auteur et les personnes visées. Cette destruction sera effectuée au plus tard trois mois après la clôture de l'ensemble des opérations de recevabilité ou de vérification de l'alerte.

8.7. Lorsqu'une procédure disciplinaire ou des poursuites judiciaires sont engagées à l'encontre d'une ou plusieurs personnes mises en cause par l'alerte, les données relatives à l'alerte sont conservées jusqu'au terme de la procédure.

## 9. LES REFERENTS ALERTES

9.1. Le Référent Alertes reçoit et analyse les alertes lui ayant été signalées par tout moyen, et notamment via le site internet sécurisé, courrier, email, téléphone ou en personne. Il peut se faire assister de délégués.

9.2. Le Référent Alertes assure le traitement confidentiel des alertes dans les conditions prévues à la Section 6 de cette Procédure, et veille à la confidentialité, à la protection et à la durée de conservation des données personnelles recueillies dans le cadre du traitement de l'alerte dans les conditions prévues à la Section 8 de cette Procédure. Il en va de même pour ses délégués.

9.3. Le Référent Alertes peut faire appel à des experts internes ou externes dans le cadre du traitement des alertes et, plus généralement, avoir recours aux différents services de l'organisation.

9.4. L'organisation veille à ce que le prestataire de service éventuellement désigné pour gérer tout ou partie de ce dispositif s'engage à ne pas utiliser les données à des fins détournées, à assurer leur confidentialité, à respecter la durée de conservation limitée des données et à procéder à la destruction ou à la restitution de tous les supports manuels ou informatisés de données à caractère personnel au terme de sa prestation.[2]

9.5. A l'issue de l'instruction d'une alerte, le Référent Alertes formule, le cas échéant, des recommandations à destination du département des ressources humaines, concernant les éventuelles sanctions disciplinaires à prendre à l'encontre des individus visés par le signalement ou de l'auteur du signalement en cas de signalement de mauvaise foi, ou toute notification éventuelle aux autorités compétentes. Les formulations utilisées pour décrire la nature des faits signalés indiquent leur caractère présumé.

9.6. Par exception à ce qui précède, le Référent Alertes porte sans délai à la connaissance du Directeur Général et/ou le comité de compliance les situations, allégations, ou signalements, dont il aurait connaissance :

9.6.1. Mettant en cause, un directeur général d'une des filiales, un membre du comité exécutif ou du conseil d'administration, et ce dans une logique de bonne gouvernance ; ou

9.6.2. Portant sur un soupçon ou une allégation de blanchiment d'argent, de corruption privée ou publique, de trafic d'influence, de fraude interne ou externe, ou d'atteinte (ou risque d'atteinte) grave aux droits humains et libertés fondamentales.

## 10. SUIVI DES ALERTES

10.1. Afin de pouvoir évaluer l'efficacité du dispositif d'alerte, le Référent Alertes peut mettre en place un suivi annuel statistique concernant la réception, le traitement et les suites données aux alertes.

10.2. Ce suivi annuel statistique peut faire apparaître le nombre d'alertes reçues, de dossiers clos, de dossiers ayant donné ou donnant lieu à une enquête, le nombre et le type de mesures prises pendant et à l'issue de l'enquête (mesures conservatoires, engagement d'une procédure disciplinaire ou judiciaire, sanctions prononcées, etc.).

## 11. DISTRIBUTION

11.1. L'organisation portera à la connaissance de ses salariés et de ses collaborateurs l'existence de leur droit d'alerte, y compris, par exemple, par voie d'affichage ou de notification.

[2]Tout transfert de données à caractère personnel hors de l'Union Européenne, vers une personne morale établie dans un pays non membre de l'Union européenne et n'accordant pas une protection suffisante au sens de l'article 68 de la loi du 6 janvier 1978 modifiée, sera opéré conformément aux dispositions spécifiques de la loi n°78-17 du 6 janvier 1978 modifiée relatives aux transferts internationaux de données ainsi que du Règlement général sur la protection des données (Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016).

## 12. CONTACT

12.1. Pour toute question relative à cette Procédure, et aux garanties encadrant le droit d'alerte, les collaborateurs internes ou externes à l'organisation sont invités à contacter :

12.1.1. complianceofficer@circet.com

12.2. Les demandes de renseignement concernant le droit d'alerte ne seront pas considérées comme un signalement entrant dans le champ du dispositif de cette Procédure.

# 2. WHISTLEBLOWING PROCEDURE

## 1. SUMMARY

1.1. In-house employees and external or casual collaborators of by the CIRCET Group (the "Organization") can report, in confidence, any serious breach of public interests or the provisions of its Code of Conduct. They must be able to inform the Organization of a possible or proven breach of statutory and regulatory provisions, or its internal procedures, to guarantee its correct functionning.

1.2. The procedure described below (the "Procedure") allows those who so wish to exercise the right to report their concerns to be protected as a whistleblower in accordance with French Act no. 2016-1691 of December 9, 2016 on transparency, preventing bribery and modernizing the economy and the terms and conditions set out in Decree no. 2017-564 of April 19, 2017.

1.3. This Procedure is optional and the Organization will not take any measures against anyone who chooses not to use it. It is not intended to act as a substitute for normal internal communications channels through the Organization's line management structure and through direct or indirect line managers, the Human Resources department, or an employee or staff representative: this is therefore a subsidiary option.

1.4. Particular precautions are taken by the Organization to manage how reports of this kind are handled, in accordance with the applicable laws and regulations, including deliberation no. 2017-191 of June 22, 2017, amending deliberation no. 2005-305 of December 8, 2005 on single authorization for automated processing of personal data implemented in the context of workplace whistleblowing (AU-004) of the CNIL (Commission Nationale Informatique et Liberté) [the French Information Commission] and following the data protection impact analysis carried out by the Organization pursuant to CNIL deliberation no. 2018-327.

## 2. WHISTLEBLOWING

2.1. Whistleblowing can be summarized as the possibility offered to anyone to decide whether or not to report a serious breach of general interest, of which they have personal knowledge.

2.2. The report may relate to a crime or misdemeanor, any serious and manifest breach of a regulation, law or international treaty ratified by France, and any threat or serious harm to the general interest[3].

2.3. The report may, for example, relate to any fact or behavior that constitutes a breach of the rules set out in laws or regulations.

2.4. Any situation that does not appear to comply with the provisions of the Organization's Code of Conduct may also be reported.

[3] Facts, information or documents in any form or on any medium, which are covered by confidentiality on the grounds of national defense, doctor-patient confidentiality or attorney-client privilege are excluded from the whistleblowing mechanism defined in this Procedure.

## 3. WHISTLEBLOWERS

3.1. All in-house employees (full-time, part-time and temporary employees, apprentices and interns) and external or casual collaborators (including subcontractors or suppliers) in the Organization are entitled to report their concerns. People involved in activities connected with, but not organized by the Organization, should report their concerns to the agency responsible for running the activity.

3.2. A whistleblower must be:

(a) A natural person,
(b) Acting in good faith,
(c) Selflessy,
(d) Reporting facts of which they have personal knowledge and
(e) Acting in accordance with the Procedure, as detailed in Section 4.

3.2.1. A whistleblower must act in good faith, i.e. have a reasonable belief that the facts are true at the time they are reported.

3.2.2. The report must be sefless, i.e. its author cannot claim any kind of remuneration, benefit or consideration, and must not act with the intention of causing harm to someone else.

3.2.3. Finally, the whistleblower must have personal knowledge of the facts they are reporting. Any report where the author does not have personal knowledge of the facts, where they have been reported by someone else, or which are based on an unsubstantiated suspicion or allegation, will be deemed inadmissible.

## 4. REPORTING A CONCERN

4.1. In-house employees can report their concerns directly to people within the Organization appointed to receive and analyze reports of this kind (known as “Prescribed Persons”) or via our whistleblowing platform, available online.

It should be noted that this is a subsidiary process and not intended to act as a substitute for normal internal communications channels through the Organization’s line management structure, such as direct or indirect line managers, the Human Resources department, or an employee or staff representative, whom employees are encouraged to contact.

4.2. Collaborators outside the Organization can report their concerns to a “Prescribed Person” or or via our whistleblowing platform, available online.

4.3. The report must contain all factual information or relevant documents to back up the claim, to ensure that it is as exhaustive, accurate, substantiated and well documented as possible; in particular, it must state when the facts occurred and the identity of those involved, if the author is aware of this information.

4.4. The whistleblower must explain how they have become personally aware of the facts and whether a third party has been informed of the facts, either by the whistleblower themselves or by any other means.

4.5. The whistleblower is invited to provide any information (such as their last name, first name and contact details) that will allow the Organization to contact them and discuss the situation, while keeping their identity confidential.

4.6. In exceptional situations, an anonymous report may be accepted, provided the gravity of the situation has been established and the factual elements are sufficiently detailed. Handling of anonymous reports will be subject to special precautions, such as a preliminary investigation by the initial recipient, or the appropriateness of disseminating it via the whistleblowing mechanism. The secure website allows but does not encourage anonymity. It is more difficult, and in some cases impossible, to investigate an anonymous report or establish whether the facts are well founded. The Organization recommends that reports are made by a named person; the investigation process is easier when the whistleblower is known, as it is then possible to talk to them, on the understanding that the Organization undertakes to maintain confidentiality.

## 5. CONFIDENTIALITY

5.1. The Organization guarantees strict confidentiality in respect of:

- 5.1.1. The whistleblower's identity,
- 5.1.2. The identity of the people named in the report,
- 5.1.3. All information gathered during the course of the investigation.

5.2. Once a report has been submitted, discussions between the Prescribed Person (and/or their deputies) and the whistleblower will take place on the plateform. Not using this system, or using other means of communication, will not affect the potential admissibility of the alert or expose its author to sanctions. Access to communications on the platform is reserved for the Prescribed Person and their deputies, if any.

5.3. If a whistleblowing report is submitted by letter, it is advisable to use the double-envelope method: all the information is placed in a sealed envelope – known as the inner envelope – which is in turn inserted into another envelope.

## 6. INVESTIGATION

6.1. Whistleblowing reports are verified, investigated and analyzed by the Organization as soon as possible, and are subject to confidentiality. The whistleblower is not advised to carry out their own investigation or to seek to establish a legal position on the facts reported.

6.2. The whistleblower will receive immediate confirmation from the platform that their report has been forwarded and must keep the code confidential. Confirmation of forwarding does not mean that the report is admissible.

6.3. An examination of admissibility will be carried out within a reasonable time frame, in principle no more than 15 working days after the report is received. The author will be kept informed of the admissibility of their report. If the report is admissible, an investigation will be carried out to determine the reality of the facts reported.

- 6.3.1. However, time frames may vary, depending on the nature of the report.

6.4. If a reasonable period of time after submitting a report has elapsed and its author has not been told whether it is admissible, they may forward it to the judicial authorities (such as a public prosecutor or judge) or an administrative body (such as a prefect, the CNIL or the French Anti-Corruption Agency (AFA)). As a last resort, if the report has not been investigated by these authorities within three months, the whistleblower may make it public (for example, by reporting it to the media, an association, a nongovernmental organization (NGO) or a trade union).

6.5. A report may only be brought directly to the attention of the relevant authorities or made public in the event of serious and imminent danger, or if there is a risk of irreversible harm.

6.5.1. Serious and imminent danger means any type of danger likely to cause injuries or death, and which is likely to occur soon.

6.6. If in doubt, anyone may communicate their concerns to the French Défenseur des droits (Defender of Rights) and be referred to the appropriate organization. Any report referred to the Defender of Rights must be sent by post in writing, in a double envelope. All the relevant information must be placed in a sealed envelope – called the inner envelope – which is then placed in a second – outer – envelope addressed to the Defender of Rights. Only the following should be written on the inner envelope: "WHISTLEBLOWING REPORT UNDER THE ACT OF DECEMBER 9, 2016 SENT ON (date of sending).” The following address should be used on the outer envelope: Défenseur des droits, Libre réponse 71120, 75342 PARIS CEDEX 07.

## 7. PROTECTION FROM REPRISALS

7.1. The Organization will protect any individual who has report, selflessy and in good faith, facts that could constitute a crime or misdemeanor, even if the facts reported subsequently prove to be inaccurate, or if no further action is taken.

7.2. No individual may be withdrawn from a recruitment procedure or denied access to an internship or period of training, and no employee may be sanctioned, dismissed or subject to any form of direct or indirect discrimination, notably in respect of compensation, profit-sharing or share allocations, training, redeployment, assignment, qualification, grading, professional promotion, transfer, or renewal of their contract.

7.3. Any employee or member of staff who believes they have been subject to reprisals for having reported or provided evidence, in good faith, of facts constituting a crime or misdemeanor, of which they have become aware during the course of their duties, may report this to the Prescribed Person or, if they are dismissed, refer the matter to an Employment Tribunal ruling in emergency proceedings.

7.4. Any misuse of the system, particularly in terms of slanderous report (namely, reporting information which one knows to be wholly or partially inaccurate) or which is done in bad faith, will render the individual concerned liable to prosecution according to French law (Article 226-10 of the French Criminal Code) and to disciplinary sanctions according to the Organization’s internal regulations.

7.5. Any employee who prevents or has previously prevented a whistleblowing report from being submitted, or who has taken action against the author of a report, may be subject to legal action or to disciplinary sanctions according to the Organization's internal regulations.

## 8. PROCESSING OF PERSONAL DATA

8.1. The Organization will only record the following information in relation to investigating a whistleblowing report:
- 8.1.1. The author's identity, duties and contact details;
- 8.1.2. The identities, duties and contact details of those named in the report;
- 8.1.3. The identities, duties and contact details of those responsible for receiving and investigating the report;
- 8.1.4. The facts reported;
- 8.1.5. Information gathered during the process of verifying the facts reported;
- 8.1.6. A report of the verification actions taken;
- 8.1.7. The follow-up to the report.
- 8.1.8. The aim of collecting and processing these personal data is to determine whether the report is admissible, verify the facts, and take any corrective measures required. This allows the Organization to comply with its statutory obligations (arising, in particular, from the so-called "Sapin 2" Act of December 9, 2016 and the law of March 27, 2017 on the duty of vigilance, and to protect its legitimate interests (by complying with the law and the Organization's ethical principles).

8.2. The right to access, rectify and object to the use of data may be exercised within the statutory and regulatory framework by contacting the Prescribed Person by email.

8.3. Under no circumstances may the person named in the report obtain information concerning the identity of the whistleblower from the data controller.

8.4. Both the whistleblower and the person named in the report may be assisted by any person of their choice from within the Organization, at any stage of the process.

8.5. Any data relating to a report that is not considered to fall under this procedure will be deleted or anonymized and archived by the Organization.

8.6. If no follow-up is required, the Organization will destroy all the evidence in the report that would identify the whistleblower or the persons named in connection with it. This must take place no later than three months after the closure of the admissibility or verification procedures relating to the report.

8.7. Where disciplinary or legal proceedings are taken against one or more persons named in the report, the data relating to it will be retained until the proceedings are complete.

## 9. PRESCRIBED PERSONS

9.1. The Prescribed Person receives and analyzes whistleblowing reports sent to them by any means, in particular via the secure website, post, email, phone, or in person. They may be assisted by one or more deputies.

9.2. The Prescribed Person will investigate reports in confidence, in accordance with the conditions set out in Section 6 of this Procedure, and will be responsible for the confidentiality, protection and retention period of personal data gathered in the process of investigating the report under the conditions set out in Section 8 of this Procedure. The same applies to their deputies.

9.3. The Prescribed Person may call on internal or external experts in the context of investigating whistleblowing reports and, more generally, have access to the Organization's various services.

9.4. The Organization will ensure that any service provider appointed to manage all or part of the system undertakes not to use the data for any unrelated purposes, ensure they are kept confidential and only retained for a limited period of time, and that all manual or electronic media containing personal data are destroyed or returned once the service has been delivered.[4]

9.5. Once a report has been investigated, the Prescribed Person will, if necessary, produce recommendations for the human resources department concerning any disciplinary sanctions to be taken against the individuals named in the report, or the author of the report if this has been submitted in bad faith, or notify the relevant authorities as necessary. The terms used to describe the nature of the facts reported must indicate that they are presumed.

9.6. As an exception to the above, the Prescribed Person will bring to the immediate attention of the Managing Director and/or the Compliance Committee any situations, allegations or reports of which they may be aware:

9.6.1. Implicating a managing director of one of the subsidiaries, a member of the Executive Committee, or a member of the Board of Directors, from the perspective of good governance; or

9.6.2. Where there is a suspicion or allegation of money laundering, bribery involving a private individual or public official, influence peddling, internal or external fraud, or a breach (or risk of a breach) of human rights and fundamental freedoms.

## 10. MONITORING

10.1. The Prescribed Person may implement annual statistical monitoring of reports received and investigated and follow-up actions, in order to assess the effectiveness of the whistleblowing system.

10.2. This may show the number of alerts received, closed cases, cases that have previously been or are currently being investigated, the number and type of measures taken during and after the investigation (such as measures to protect evidence, disciplinary or judicial proceedings, sanctions imposed, etc.).

[4] Any transfer of personal data outside the European Union, to a legal entity based in a country that is not a member of the European Union and that does not provide adequate protection as defined in Article 68 of the French Data Protection Act of January 6, 1978 as amended, will be carried out in accordance with the specific provisions of French Act no. 78-17 of January 6, 1978 as amended on international data transfers and with the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016).

## 11. DISTRIBUTION

11.1. The Organization will make its staff and other employees aware of their right to report their concerns, including, for example, by putting up posters or notifying them directly.

## 12. CONTACT

12.1. Employees both inside and outside the Organization are invited to contact the following if they have any questions about this Procedure or the guarantees governing their rights on whistleblowing:

12.1.1. complianceofficer@circet.com

12.2. Requests for information about rights on whistleblowing will not be treated as a whistleblowing report covered by the scope of this Procedure.

# 3. PROCEDIMIENTO RELATIVO A LOS DENUNCIANTES

## 1. RESUMEN

Los empleados y colaboradores externos u ocasionales del Grupo CIRCET (en adelante, la "Organización") podrán comunicarle, de manera confidencial, cualquier violación grave del interés general y de las disposiciones de su código de conducta. El buen funcionamiento de la organización requiere que sean capaces de informar a la organización de un incumplimiento, posible o probado, de las disposiciones legales y reglamentarias, así como de los procedimientos internos.

El procedimiento que se describe a continuación (en adelante, el "Procedimiento") permite a aquellos que así lo deseen ejercer su derecho de avisar y beneficiarse de la protección de los denunciantes de irregularidades prevista en la ley n.º 2016-1691, del 9 de diciembre de 2016, relativa a la transparencia, la lucha contra la corrupción y la modernización de la vida económica, y de conformidad con las condiciones establecidas en el decreto n.º 2017-564, del 19 de abril de 2017.

Este procedimiento es opcional y la Organización no tomará ninguna medida contra quienes no lo utilicen. No tiene por objeto sustituir los canales normales de comunicación interna a través de la estructura jerárquica de la Organización y del superior jerárquico directo o indirecto, el Departamento de Recursos Humanos, o un empleado o representante del personal: tiene, por tanto, un carácter subsidiario.

La Organización ha previsto precauciones especiales para supervisar la tramitación de esas denuncias, de conformidad con las leyes y reglamentos aplicables, incluida la deliberación n.º 2017-191 del 22 de junio de 2017, que modifica la deliberación n.º 2005-305 del 8 de diciembre de 2005, relativa a la autorización única del tratamiento automatizado de datos de carácter personal aplicada en el contexto de los sistemas de denuncia profesional (AU-004) de la Comisión Nacional de Informática y Libertades (CNIL) francesa y como resultado de las directrices sobre la evaluación de impacto relativas a la protección de datos (AIPD) realizada por la Organización con arreglo a la deliberación n.º 2018-327 de la CNIL.

## 2. EL DERECHO DE DENUNCIA

2.1. El derecho de denuncia puede resumirse como el derecho de toda persona a decidir si denunciar o no una infracción grave de interés público de la que tiene conocimiento personal.

2.2. La denuncia puede referirse a cualquier crimen o delito, a cualquier infracción grave y manifiesta de un reglamento, ley o tratado internacional ratificado por Francia, o a cualquier amenaza o perjuicio grave para el interés general[5].

2.3. Por ejemplo, la denuncia puede referirse a cualquier hecho o comportamiento que constituya una infracción de las normas de las leyes y reglamentos.

[5] Los hechos, informaciones o documentos, en cualquier forma o soporte en el que se presenten, amparados por el secreto de defensa nacional, el secreto médico o el secreto de las relaciones entre un abogado y su cliente, quedan excluidos del sistema de denuncia definido por este Procedimiento.

2.4. También se puede informar de cualquier situación que no se ajuste a lo dispuesto en el código de conducta de la Organización.

## 3. EL DENUNCIANTE

3.1. Todos los empleados internos (a tiempo completo, a tiempo parcial, empleados temporales, aprendices y becarios), así como los empleados externos u ocasionales (incluidos los subcontratistas o proveedores) de la Organización pueden presentar una denuncia. Se invita a las personas que participen en actividades relacionadas con la Organización, pero no organizadas por ella, a que presenten su denuncia en el organismo que organiza la actividad.

3.2. Para presentar una denuncia, tiene que cumplir los siguientes requisitos:

(a) ser una persona física,
(b) actuar de buena fe,
(c) actuar de manera desinteresada,
(d) informar de los hechos de los que ha tenido conocimiento en persona y
(e) respetar el Procedimiento que se describe en la Sección 4.

3.2.1. La denuncia debe hacerse de buena fe, es decir, con la creencia razonable de que los hechos son verdaderos en el momento de la presentación de la denuncia.

3.2.2. La denuncia debe ser desinteresada, es decir, la persona que la presenta no reclama ninguna remuneración, beneficio o consideración, y no actúa con la intención de perjudicar a otros.

3.2.3. Por último, el denunciante debe conocer en persona los hechos que denuncia. Se considerarán inadmisibles las denuncias de hechos que no se conozcan personalmente, que se conozcan a través de otra persona o que se basen en una sospecha o alegación no fundamentada.

## 4. PRESENTAR UNE DENUNCIA

4.1. Los empleados internos de la organización pueden informar directamente a los coordinadores especialmente designados por la Organización para recibir y analizar las denuncias (en adelante, los "Coordinadores de denuncias") al igual que a través de nuestra plataforma de denuncias, a la que puede accederse online.

Se recuerda que este procedimiento tiene un carácter subsidiario y que no sustituye a los canales normales de comunicación interna a través de la estructura jerárquica de la Organización, por lo que todos, tanto el superior jerárquico directo o indirecto, el Departamento de Recursos Humanos, o un empleado o representante del personal como los colaboradores internos, podrán hacer uso de él.

4.2. Los empleados externos de la Organización pueden presentar denuncias a través de los Coordinadores de denuncias, así como a través de nuestra plataforma de denuncias a la que puede accederse online.

4.3. La denuncia debe incluir todos los hechos, información o documentos pertinentes que la fundamenten, de modo que sea lo más completa, exacta, detallada y esté lo mejor

documentada posible; en particular, la denuncia debe especificar la fecha en que se produjeron los hechos y la identidad de las personas involucradas cuando estos elementos sean conocidos por el autor de la denuncia.

4.4. El autor especificará las razones de su conocimiento personal de los hechos y si el denunciante o cualquier otra persona ha informado a algún tercero de lo sucedido.

4.5. Se invita al autor de la denuncia a que facilite cualquier información que permita a la Organización, preservando la confidencialidad de su identidad, ponerse en contacto con él (apellidos, nombres, datos de contacto) y hablar sobre la denuncia.

4.6. Como excepción, se podrá tramitar una denuncia anónima siempre que se establezca la gravedad de los hechos mencionados y que los elementos de hecho hayan quedado suficientemente detallados. La tramitación de esta denuncia estará rodeada de precauciones específicas, como un examen preliminar por parte de su primer destinatario, o incluso la conveniencia de su difusión en el marco del sistema. El sitio web dedicado permite el anonimato, pero no lo fomenta. Es más difícil, y a veces imposible, procesar una denuncia anónima o determinar si los hechos son verdaderos. La Organización recomienda que la denuncia sea nominativa, ya que se facilita el proceso de investigación cuando se conoce la identidad del autor de la infracción para poder comentarla con él o ella, teniendo en cuenta que la Organización se compromete a mantener la confidencialidad.

## 5. CONFIDENCIALIDAD

5.1. La Organización garantiza la estricta confidencialidad de lo siguiente:
- 5.1.1. La identidad del autor de una denuncia.
- 5.1.2. La identidad de las personas implicadas en la denuncia.
- 5.1.3. De toda la información recogida en el contexto de la tramitación de la denuncia.

5.2. Una vez que se ha recogido la denuncia, el intercambio entre los Coordinadores de denuncias (y/o sus posibles delegados) y el autor de la denuncia se realiza a través de la plataforma de denuncias. El hecho de que no se recurra a este sistema de mensajería o al uso de otros medios de comunicación no afecta a la posible admisibilidad de la denuncia, ni expone a su autor a sanciones. El acceso al sistema de mensajería de la plataforma está reservado para los Coordinadores de denuncias y sus posibles delegados.

5.3. En el caso de presentar una denuncia por correo, se recomienda utilizar el método del doble sobre: todos los elementos de la denuncia en un sobre cerrado (llamado sobre interior) que a su vez se introducirá en un segundo sobre.

## 6. TRAMITACIÓN DE LAS DENUNCIAS

6.1. La verificación, la tramitación y el análisis de las denuncias los lleva a cabo la Organización lo antes posible y en cumplimiento del carácter confidencial de la denuncia No se aconseja que el autor de la denuncia lleve a cabo su propia investigación, ni que trate de establecer la calificación jurídica de los hechos denunciados.

6.2. El autor de la denuncia recibirá inmediatamente a través de la plataforma una confirmación de la transmisión de su denuncia y tendrá que guardar su código confidencial. La confirmación de

que se haya transmitido correctamente no debe interpretarse como la admisibilidad de la denuncia.

6.3. El examen de la admisibilidad de la denuncia se efectuará en un plazo razonable que no excederá, en principio, de 15 días laborables a partir de la recepción de la denuncia. Se informará al autor sobre la admisibilidad. Si la denuncia es admisible, se llevará a cabo una investigación para determinar la realidad de los hechos denunciados.
   6.3.1. Sin embargo, los plazos pueden variar dependiendo de los elementos denunciados.

6.4. Si, transcurrido un plazo razonable después de haber comunicado una denuncia, el autor no ha recibido ninguna confirmación sobre su admisibilidad, podrá enviar la denuncia a las autoridades judiciales (por ejemplo, el fiscal, el juez, etc.) o administrativas (por ejemplo, la prefectura; la Comisión Nacional de Informática y Libertades [CNIL], la Agencia Francesa Anticorrupción [AFA]). Como último recurso y si la denuncia no es atendida por ninguna de estas autoridades en un plazo de tres meses, el autor de la denuncia puede hacerla pública (por ejemplo: presentar la denuncia ante los medios de comunicación, una asociación, una ONG o un sindicato).

6.5. La denuncia puede presentarse directamente a las autoridades competentes o hacerse pública solo en caso de peligro grave e inminente o cuando exista un riesgo de daño irreversible.
   6.5.1. Por peligro grave e inminente se entiende cualquier tipo de peligro que pueda provocar lesiones o la muerte y vaya a tener lugar de forma inminente.

6.6. En caso de duda, cualquier persona puede dirigir su denuncia al Defensor de los Derechos Humanos para que este lo remita al organismo apropiado para que se tramite la denuncia. La presentación de una denuncia ante el Defensor de los Derechos Humanos se le enviará por escrito en doble sobre por correo. Todos los elementos de la remisión deben introducirse en un sobre cerrado, el llamado sobre interior, que se introducirá en un segundo sobre dirigido al Defensor de los Derechos Humanos, el llamado sobre exterior. El sobre interior solo incluirá el siguiente texto: "NOTIFICACIÓN DE UNA DENUNCIA DE CONFORMIDAD CON LA LEY DEL 9 DE DICIEMBRE DE 2016 CON FECHA DE (fecha del envío)". En el sobre exterior figurará la dirección siguiente: Défenseur des droits, Libre réponse 71120, 75342 PARIS CEDEX 07.

## 7. PROTECCIÓN CONTRA REPRESALIAS

7.1. La Organización protege a toda persona que haya puesto en su conocimiento, de manera desinteresada y de buena fe, hechos que constituyan una falta o un delito, aunque los hechos denunciados resulten ser inexactos o no den lugar a ninguna acción.

7.2. No podrá excluirse a ninguna persona de un procedimiento de contratación o del acceso a un curso o período de formación, ni ningún empleado podrá ser sancionado, despedido o ser objeto de una medida discriminatoria directa o indirecta, en particular en materia de remuneración, medidas de participación en los beneficios o distribución de acciones, formación, reclasificación, asignación, calificación, clasificación, promoción profesional, traslado o renovación de contrato.

7.3. Todo empleado o colaborador que considere que ha sido objeto de represalias por haber denunciado o testificado, de buena fe, hechos constitutivos de una falta o un delito de los que

hubiera tenido conocimiento en el ejercicio de sus funciones, podrá comunicarlo a los Coordinadores de denuncias o remitir el asunto al tribunal laboral en caso de despido.

7.4. odo uso indebido del sistema, en particular en forma de denuncia calumniosa (presentación de información de la que se sabe que es total o parcialmente inexacta) o hecha de mala fe expone al autor a ser denunciado ante un tribunal con arreglo a la ley (artículo 226-10 del código penal francés) y, de conformidad con el Reglamento Interno, a verse expuesto a medidas disciplinarias.

7.5. Todo empleado que obstruya o haya obstruido la transmisión de una denuncia, o que haya tomado medidas de represalia contra el autor de una denuncia, podrá ser objeto de un procedimiento judicial y podrá, de conformidad con el Reglamento Interno, ser objeto de medidas disciplinarias.

## 8. TRATAMIENTO DE LOS DATOS PERSONALES

8.1. La Organización solo registra los siguientes datos al procesar una denuncia:

8.1.1. identidad, funciones y datos de contacto de la persona que presenta la denuncia;
8.1.2. identidad, funciones y datos de contacto de las personas objeto de una denuncia;
8.1.3. identidad, funciones y datos de contacto de las personas que participan en la tramitación o el procesamiento de la denuncia;
8.1.4. hechos denunciados;
8.1.5. pruebas reunidas en el trascurso de la verificación de los hechos denunciados;
8.1.6. informe de las operaciones de verificación;
8.1.7. respuesta a la denuncia.

La finalidad de la recopilación y el tratamiento de esos datos personales es determinar la admisibilidad de los informes, verificar los hechos y adoptar medidas correctivas en caso necesario. De este modo, permiten que la Organización respete sus obligaciones legales (en virtud de la ley denominada "Sapin 2", del 9 de diciembre de 2016, y de la ley del 27 de marzo de 2017 relativa al deber de vigilancia) y proteja sus intereses legítimos (respetando la ley y los principios éticos de la Organización).

8.2. El derecho de acceso, rectificación y oposición al uso de los datos podrá ejercerse, dentro del marco legal y reglamentario, poniéndose en contacto con el Coordinador de denuncias en la dirección.

8.3. La persona objeto de la denuncia no podrá, en ningún caso, obtener del responsable del tratamiento ninguna información relativa a la identidad del autor de la denuncia.

8.4. El emisor de la denuncia o la persona objeto de la misma podrá ser asistido por cualquier persona de su elección dentro de la Organización durante todas las etapas del proceso.

8.5. Cualquier dato relativo a una denuncia que se considere fuera del ámbito de la parte operativa de este procedimiento será eliminado o archivado tras la anonimización por parte de la Organización.

8.6. Si no se toma ninguna medida en relación con una denuncia, la Organización destruirá todos los elementos del archivo de la denuncia que identifiquen al autor y a las personas involucradas.

Esta destrucción se llevará a cabo, como máximo, tres meses después de la clausura de todas las operaciones de admisibilidad o verificación de la denuncia.

8.7. Cuando se inicien procedimientos disciplinarios o judiciales contra una o más personas implicadas en la denuncia, los datos relativos a la misma se conservarán hasta el final del procedimiento.

## 9. LOS COORDINADORES DE DENUNCIAS

9.1. El Coordinador de denuncias recibe y analiza las denuncias que le han sido comunicadas por cualquier medio, y en particular, a través del sitio web seguro, el correo, el correo electrónico, el teléfono o en persona. Puede recibir la ayuda de delegados.

9.2. Las descripciones del Coordinador de denuncias garantizarán el tratamiento confidencial de las descripciones en las condiciones previstas en la Sección 6 del presente Procedimiento, y asegurarán la confidencialidad, la protección y el período de conservación de los datos personales recogidos en el contexto del tratamiento de la descripción en las condiciones previstas en la Sección 8 del presente Procedimiento. Lo mismo ocurre con sus delegados.

9.3. El Coordinador de denuncias puede recurrir a expertos internos o externos para la tramitación de las denuncias y, de manera más general, utilizar los diferentes servicios de la Organización.

9.4. La Organización se asegurará de que todo proveedor de servicios que pueda ser designado para gestionar todo o parte de este sistema se comprometa a no utilizar los datos con fines indebidos, a garantizar su confidencialidad, a respetar el período de retención limitado de los datos y a destruir o devolver todos los soportes de datos personales manuales o informatizados al final de su servicio.[6]

9.5. Tras la investigación de una denuncia, el Coordinador de denuncias formula, cuando procede, recomendaciones al Departamento de Recursos Humanos sobre las posibles medidas disciplinarias que deben adoptarse contra las personas objeto de la denuncia o el autor de la misma en caso de una denuncia presentada de mala fe, o sobre cualquier posible notificación a las autoridades competentes. Las fórmulas utilizadas para describir la naturaleza de los hechos denunciados indican su carácter de presunción.

9.6. Como excepción a lo anterior, los Coordinadores de denuncias informarán de inmediato al director general y/o al Comité de cumplimiento de cualquier situación, alegación o informe del que tengan conocimiento:

9.6.1. que implique a un director general de alguna de las filiales, un miembro del comité ejecutivo o de la junta directiva, todo ello en un contexto de buena gestión; o

9.6.2. que esté relacionado con una sospecha o alegación de blanqueo de dinero, corrupción privada o pública, tráfico de influencias, fraude interno o externo, o infracción grave (o riesgo de infracción) de los derechos humanos y las libertades fundamentales.

[6] Toda transferencia de datos de carácter personal fuera de la Unión Europea, a una persona jurídica establecida en un país que no sea miembro de la Unión Europea y que no ofrezca una protección suficiente en el sentido del artículo 68 de la ley del 6 de enero de 1978 modificada, se efectuará de conformidad con las disposiciones específicas de la ley n.º 78-17, del 6 de enero de 1978, modificada, relativa a las transferencias internacionales de datos, y del Reglamento General de Protección de Datos (Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, del 27 de abril de 2016).

## 10. SEGUIMIENTO DE LA DENUNCIA

10.1. Para poder evaluar la eficacia del sistema de denuncias, el Coordinador de denuncias puede establecer un seguimiento estadístico anual de la recepción, la tramitación y el seguimiento de las denuncias.

10.2. Este seguimiento estadístico anual puede mostrar el número de denuncias recibidas, los casos cerrados, los casos que han dado lugar o estén dando lugar a una investigación, el número y el tipo de medidas adoptadas durante y al final de la investigación (medidas cautelares, iniciación de procedimientos disciplinarios o judiciales, sanciones impuestas, etc.).

## 11. DISTRIBUCIÓN

11.1. La Organización dará a conocer a sus empleados y colaboradores la existencia de su derecho a denunciar, por ejemplo, mediante publicaciones o notificaciones.

## 12. CONTACTO

12.1. Para cualquier cuestión relativa a este Procedimiento, y a las garantías que rigen el derecho a la denuncia, se invita a los empleados internos o externos de la Organización a que se pongan en contacto con:

12.1.1. complianceofficer@circet.com

12.2. Las investigaciones relativas al derecho a la denuncia no se considerarán como una denuncia comprendida en el ámbito de la parte dispositiva de este Procedimiento.

# 4. WHISTLEBLOWER-VERFAHREN

## 1. KURZFASSUNG

1.1. Mitarbeiter und externe oder gelegentliche Mitarbeiter der CIRCET-Gruppe („die Organisation“) haben die Möglichkeit, der Organisation jeden schwerwiegenden Verstoß gegen das Interesse der Allgemeinheit und die Bestimmungen ihres Verhaltenskodexes auf vertrauliche Weise zur Kenntnis zu bringen. Das ordnungsgemäße Funktionieren der Organisation setzt voraus, dass diese Personen in der Lage sind, die Organisation über einen möglichen oder erwiesenen Verstoß gegen gesetzliche und behördliche Bestimmungen sowie interne Verfahren zu informieren.

1.2. Das nachstehend beschriebene Verfahren (das „Verfahren“) ermöglicht es denjenigen, die dies wünschen, ihr Whistleblowing-Recht auszuüben und den Schutz von Whistleblowern in Anspruch zu nehmen, der im Französischen Gesetz Nr. 2016-1691 vom 9. Dezember 2016 über Transparenz, Korruptionsbekämpfung und Modernisierung des Wirtschaftslebens und in Übereinstimmung mit den im Erlaß Nr. 2017-564 vom 19. April 2017 festgelegten Bedingungen vorgesehen ist.

1.3. Dieses Verfahren ist optional und die Organisation wird keine Maßnahmen gegen diejenigen ergreifen, die es nicht anwenden. Es ist nicht beabsichtigt, die normalen Kanäle der internen Kommunikation zu ersetzen, die über die hierarchische Struktur der Organisation mit dem direkten oder indirekten hierarchischen Vorgesetzten, der Personalabteilung oder einem Belegschafts- oder Personalvertreter organisiert sind. Es ist daher subsidiärer Natur.

1.4. Die Organisation hat besondere Vorkehrungsmaßnahmen zur Überwachung dieser Hinweise in Übereinstimmung mit den geltenden Gesetzen und Vorschriften getroffen, einschließlich des Beschlusses Nr. 2017-191 vom 22. Juni 2017 zur Änderung des Beschlusses Nr. 2005-305 vom 8. Dezember 2005 über die einmalige Genehmigung der automatisierten Verarbeitung personenbezogener Daten, die im Rahmen professioneller Hinweisgebersysteme (AU-004) der CNIL (Commission Nationale Informatique et Liberté) und im Anschluss an die von der Organisation gemäß dem Beschluss Nr. 2018-327 der CNIL durchgeführte Datenschutzfolgenabschätzung (AIPD) erfolgt.

## 2. DAS WHISTLEBLOWING-RECHT

2.1. Das Whistleblowing-Recht lässt sich zusammenfassen als das Recht jeder Person, zu entscheiden, ob sie eine schwerwiegende Verletzung des Interesses der Allgemeinheit, von der sie persönlich Kenntnis hat, meldet oder nicht.

2.2. Das Whistleblowing kann jedes Verbrechen oder Vergehen, jede schwere und offenkundige Verletzung einer Verordnung, eines Gesetzes oder eines von Frankreich ratifizierten internationalen Vertrags sowie jede Bedrohung oder schwere Beeinträchtigung des Interesses der Allgemeinheit betreffen[7].

[7] Tatsachen, Informationen oder Dokumente, unabhängig von ihrer Form oder ihrem Träger, die unter das Geheimnis der Landesverteidigung, das Arztgeheimnis oder das Geheimnis der Beziehungen zwischen einem Rechtsanwalt und seinem Mandanten fallen, sind von dem durch dieses Verfahren definierten Whistleblowing-Verfahren ausgeschlossen.

2.3. Das Whistleblowing kann sich zum Beispiel auf jede Tatsache oder Verhaltensweise beziehen, die eine Verletzung der Regeln von Gesetzen und Vorschriften darstellt.

2.4. Jede Situation, die nicht den Bestimmungen des Verhaltenskodex der Organisation zu entsprechen scheint, kann ebenfalls gemeldet werden.

## 3. DES WHISTLEBLOWER

3.1. Alle internen Mitarbeiter (Vollzeit-, Teilzeit- und Zeitarbeitskräfte, Auszubildende und Praktikanten) sowie externe oder gelegentliche Mitarbeiter (einschließlich Subunternehmer oder Lieferanten) der Organisation können einen Hinweis geben. Personen, die an Aktivitäten teilnehmen, die mit der Organisation in Verbindung stehen, aber nicht von der Organisation organisiert werden, sind eingeladen, ihre Hinweise der Organisation zu melden, die die Aktivität organisiert.

3.2. Whistleblower müssen:
(a) eine natürliche Person sein,
(b) in gutem Glauben handeln,
(c) uneigennützig sein,
(d) Tatsachen melden, von denen sie persönlich Kenntnis haben und
(e) das in Abschnitt 4 beschriebene Verfahren beachten.

3.2.1. Die Meldung muss in gutem Glauben erstellt werden, d. h. in der begründeten Annahme, dass die Fakten zum Zeitpunkt der Berichterstattung der Wahrheit entsprechen.

3.2.2. Der Bericht muss uneigennützig sein, d. h. die Person, die den Bericht verfasst, beansprucht keine Vergütungen, Vorteile oder Gegenleistungen und handelt nicht in der Absicht, anderen zu schaden.

3.2.3. Schließlich muss der Hinweisgeber persönliche Kenntnis von den von ihm gemeldeten Tatsachen gehabt haben. Berichte über Tatsachen, von denen man keine persönliche Kenntnis hat, die von einer anderen Person gemeldet wurden oder die auf einem unbegründeten Verdacht oder einer unbegründeten Anschuldigung beruhen, werden als unzulässig betrachtet.

## 4. HINWEIS GEBEN

4.1. Die internen Mitarbeiter der Organisation können sich direkt an die von der Organisation speziell für die Entgegennahme und Analyse von Whistleblower-Hinweisen bestimmten Referenten (**die** „Whistleblower-Referenten“) wenden und ihre Hinweise auch über unsere Meldeplattform abgeben, online verfügbar.

Es ist zu beachten, dass dieser Prozess subsidiär ist und nicht die normalen internen Kommunikationskanäle ersetzt, die über die hierarchische Struktur der Organisation stattfinden, wie z. B. den direkten oder indirekten Vorgesetzten, die Personalabteilung oder einen Belegschafts- oder Personalvertreter, zu deren Nutzung interne Mitarbeiter eingeladen werden.

4.2. Mitarbeiter von außerhalb der Organisation können sich bei den Whistblower-Referenten melden, aber auch über unsere Meldeplattform, online verfügbar.

4.3. Der Hinweis muss alle sachdienlichen Fakten, Informationen oder Dokumente zur Begründung des Hinweises enthalten, damit der Hinweis so vollständig, genau, detailliert und dokumentiert wie möglich ist. Insbesondere muss der Hinweis das Datum, an dem der Sachverhalt eingetreten ist, und die Identität der beteiligten Personen angeben, wenn diese Elemente dem Hinweisgeber bekannt sind.

4.4. Der Hinweisgeber gibt die Gründe für seine persönliche Kenntnis des Sachverhalts an und ob ein Dritter vom Hinweisgeber oder auf andere Weise über denselben Sachverhalt informiert wurde.

4.5. Der Hinweisgeber wird gebeten, alle Informationen anzugeben, die es der Organisation ermöglichen, mit ihm in Kontakt zu treten (Name, Vorname, Kontaktdaten) und den Hinweis zu besprechen. Seine Identität wird vertraulich behandelt.

4.6. Ausnahmsweise kann ein anonymer Hinweis bearbeitet werden, sofern die Schwere der genannten Tatsachen festgestellt wird und die Tatsachenelemente hinreichend detailliert sind. Die Bearbeitung dieses Hinweises wird von besonderen Vorsichtsmaßnahmen begleitet, wie z. B. einer Vorprüfung durch den ersten Empfänger oder der Angemessenheit ihrer Verbreitung im Rahmen des Systems. Die sichere Website lässt Anonymität zu, fördert sie aber nicht. Es ist schwieriger und manchmal unmöglich, einen anonymen Hinweis zu bearbeiten oder den Wahrheitsgehalt der Tatsachen festzustellen. Die Organisation empfiehlt, dass der Hinweis unter Angabe des Namens erfolgt, da der Ermittlungsprozess erleichtert wird, wenn die Identität des Hinweisgebers bekannt ist.

## 5. VERTRAULICHKEIT

5.1. Die Organisation garantiert die strenge Vertraulichkeit folgender Daten:
- 5.1.1. Identität des Hinweisgebers,
- 5.1.2. Identität der vom Hinweis betroffenen Personen,
- 5.1.3. Informationen, die im Laufe der Bearbeitung des Hinweises gesammelt wurden.

5.2. Sobald der Hinweis eingetroffen ist, erfolgt der Austausch zwischen dem Whistleblower-Referenten (und/oder seinen möglichen Beauftragten) und dem Hinweisgeber über die Meldeplattform. Ein fehlender Rückgriff auf dieses Nachrichtenübermittlungssystem oder die Verwendung anderer Kommunikationsmittel beeinträchtigt weder die mögliche Zulässigkeit des Hinweises, noch setzt es den Hinweisgeber Sanktionen aus. Der Zugang zum Nachrichtenübermittlungssystem der Meldeplattform ist dem Whistleblower-Referenten und seinen eventuellen Beauftragten vorbehalten.

5.3. Im Falle eines per Post übermittelten Hinweises wird empfohlen, die Methode des doppelten Briefumschlags zu verwenden: Alle Elemente des Hinweises werden in einen geschlossenen Umschlag – den sogenannten inneren Umschlag – gesteckt, der seinerseits in einen zweiten Umschlag gesteckt wird.

## 6. BEARBEITUNG DER HINWEISE

6.1. Die Überprüfung, Bearbeitung und Analyse von Hinweisen werden von der Organisation so schnell wie möglich und unter Beachtung der Vertraulichkeit des Hinweises durchgeführt. Der

Hinweisgeber wird nicht aufgefordert, eine eigene Untersuchung durchzuführen oder zu versuchen, die rechtliche Qualifikation der gemeldeten Sachverhalte festzustellen.

6.2. Der Hinweisgeber erhält über die Plattform sofort eine Bestätigung über die Übermittlung seines Hinweises und muss seinen Geheimcode vertraulich behandeln. Die Bestätigung der korrekten Übermittlung stellt keine Bestätigung der Zulässigkeit des Hinweises dar.

6.3. Die Prüfung der Zulässigkeit des Hinweises erfolgt innerhalb einer angemessenen Frist, die grundsätzlich 15 Arbeitstage nach Eingang des Hinweises nicht überschreiten darf. Der Hinweisgeber wird über die Zulässigkeit informiert. Wenn der Hinweis zulässig ist, wird eine Untersuchung durchgeführt, um die Realität des gemeldeten Sachverhalts festzustellen.
   6.3.1. Die Fristen können jedoch je nach den Elementen des Hinweises variieren.

6.4. Ist der Hinweisgeber nach Ablauf einer angemessenen Frist ab Eingang eines Hinweises nicht über deren Zulässigkeit informiert worden, kann er den Hinweis an die Justiz- (z. B. Staatsanwalt, Richter) oder Verwaltungsbehörden (z. B. Regionalbehörden, Datenschutzverband, Behörde zur Korruptionsbekämpfung) weiterleiten. Als letztes Mittel und wenn der Hinweis nicht innerhalb von drei Monaten von einer dieser Behörden bearbeitet wird, kann der Hinweisgeber die Information öffentlich machen (z. B. an Medien, einen Verband, eine NGO oder eine Gewerkschaft melden).

6.5. Der Hinweis darf nur bei ernster und unmittelbarer Gefahr oder bei Gefahr eines irreversiblen Schadens den zuständigen Behörden direkt zur Kenntnis gebracht oder veröffentlicht werden.
   6.5.1. Als ernste und unmittelbare Gefahr gilt jede Art von Gefahr, die wahrscheinlich zu Verletzungen oder zum Tod führt und unmittelbar bevorsteht.

6.6. Im Zweifelsfall kann jede Person ihren Hinweis an die Ombudsstelle richten, damit er an die für die Erhebung des Hinweises zuständige Stelle weitergeleitet wird. Die Meldung eines Whistleblower-Hinweises bei der Ombudsstelle wird ihr schriftlich in einem doppelten Briefumschlag per Post zugestellt. Alle Elemente dieser Meldung müssen in einen verschlossenen Umschlag – den sogenannten inneren Umschlag – gesteckt werden, der in einen zweiten, an die Ombudsstelle adressierten Umschlag, den so genannten äußeren Umschlag, gesteckt wird. Der innere Umschlag darf nur den folgenden Vermerk tragen: SIGNALEMENT D'UNE ALERTE AU TITRE DE LA LOI DU 9 DECEMBRE 2016 EFFECTUE LE (MELDUNG EINES HINWEISES GEMÄSS DEM GESETZ VOM 9. DEZEMBER 2016, DURCHGEFÜHRT AM) (Datum der Absendung). Auf dem äußeren Umschlag ist die Adresse zu verzeichnen: Défenseur des droits, Libre réponse 71120, 75342 PARIS CEDEX 07.

## 7. SCHUTZ VOR REPRESSALIEN

7.1. Die Organisation schützt jede Person, die ihr uneigennützig und in gutem Glauben Tatsachen zur Kenntnis gebracht hat, die ein Vergehen oder ein Verbrechen darstellen, selbst wenn sich die gemeldeten Tatsachen als unrichtig erweisen oder keinen Anlass zu einer Klage geben sollten.

7.2. Keine Person darf von einem Einstellungsverfahren oder vom Zugang zu einem Ausbildungskurs oder Ausbildungsabschnitt ausgeschlossen werden, und kein Mitarbeiter darf bestraft oder entlassen werden oder Gegenstand einer direkten oder indirekten diskriminierenden

Maßnahme sein, insbesondere in Bezug auf Vergütung, Gewinnbeteiligungsmaßnahmen oder die Verteilung von Aktien, Ausbildung, Neueinstufung, Zuweisung, Qualifikation, Einstufung, beruflichen Aufstieg, Versetzung oder Vertragsverlängerung.

7.3. Angestellte oder Mitarbeiter, die der Ansicht sind, dass sie Gegenstand von Repressalien waren, weil sie in gutem Glauben über Tatsachen berichtet oder ausgesagt haben, die ein Vergehen oder ein Verbrechen darstellen, von denen sie bei der Ausübung ihres Amtes Kenntnis erhalten hätten, können dies bei den „Whistleblower-Referenten“ melden oder im Falle einer Entlassung das Arbeitsgericht anrufen.

7.4. Jeder Missbrauch des Systems, insbesondere in Form von verleumderischer (Informationen, von denen bekannt ist, dass sie ganz oder teilweise unrichtig sind) oder in böser Absicht durchgeführter Meldung, setzt den Täter einer Strafverfolgung nach dem Gesetz (Artikel 226-10 des Strafgesetzbuches) und, in Übereinstimmung mit der Geschäftsordnung, Disziplinarmaßnahmen aus.

7.5. Mitarbeiter, die die Übermittlung eines Hinweises behindern oder behindert haben oder Vergeltungsmaßnahmen gegen den Hinweisgeber ergriffen haben, sind gerichtlich belangbar und können nach Maßgabe der Geschäftsordnung disziplinarisch belangt werden.

## 8. VERARBEITUNGPERSONENBEZOGENER DATEN

8.1. Die Organisation zeichnet bei der Bearbeitung eines Hinweises nur die folgenden Daten auf:

- 8.1.1. Identität, Funktionen und Kontaktdaten des Hinweisgebers,
- 8.1.2. Identität, Funktionen und Kontaktdaten der von einem Hinweis betroffenen Personen,
- 8.1.3. Identität, Funktionen und Kontaktangaben der Personen, die an der Erhebung oder Bearbeitung des Hinweises beteiligt sind;
- 8.1.4. Sachverhalt;
- 8.1.5. Beweise, die bei der Überprüfung der berichteten Fakten gesammelt wurden;
- 8.1.6. Berichterstattung;
- 8.1.7. Folgenmaßnahmen des Hinweises.

Der Zweck der Erhebung und Verarbeitung dieser personenbezogenen Daten besteht darin, die Zulässigkeit der Berichte festzustellen, die Fakten zu überprüfen und gegebenenfalls Korrekturmaßnahmen zu ergreifen. Sie ermöglichen es der Organisation somit, ihren rechtlichen Verpflichtungen nachzukommen (die sich insbesondere aus dem Französischen Gesetz „Sapin 2“ vom 9. Dezember 2016 und dem Gesetz vom 27. März 2017 über die Wachsamkeitspflicht ergeben) und ihre legitimen Interessen zu schützen (indem sie das Gesetz und die ethischen Grundsätze der Organisation respektieren).

8.2. Das Recht auf Auskunft zu, Berichtigung und Widerspruch gegen die Verwendung von Daten kann innerhalb des rechtlichen und regulatorischen Rahmens bei Whistleblower-Referenten ausgeübt werden.

8.3. Unter keinen Umständen darf die Person, die Gegenstand eines Hinweises ist, von dem für die Verarbeitung Verantwortlichen Informationen über die Identität des Hinweisgebers erhalten.

8.4. Der Hinweisgeber oder die Person, die Gegenstand eines Hinweises ist, kann in allen Schritten des Systems von einer Person ihrer Wahl innerhalb der Organisation unterstützt werden.

8.5. Alle Daten im Zusammenhang mit einem Hinweis, die außerhalb des Geltungsbereichs des operativen Teils dieses Verfahrens betrachtet würden, werden nach der Anonymisierung durch die Organisation gelöscht oder archiviert.

8.6. Wenn bei einem Hinweis nichts unternommen wird, vernichtet die Organisation alle Elemente der Hinweisunterlagen, die den Hinweisgeber und die beteiligten Personen identifizieren. Diese Vernichtung wird spätestens drei Monate nach Abschluss aller Zulässigkeits- oder Überprüfungsvorgänge des Hinweises durchgeführt.

8.7. Wird gegen eine oder mehrere vom Hinweis betroffene Personen ein Disziplinarverfahren oder ein Gerichtsverfahren eingeleitet, so werden die Daten im Zusammenhang mit dem Hinweis bis zum Abschluss des Verfahrens aufbewahrt.

## 9. REFERENTEN

9.1. Der Whistleblower-Referent erhält und analysiert die Hinweise, die ihm auf irgendeinem Wege, insbesondere über die sichere Website, per Post, E-Mail, Telefon oder persönlich gemeldet wurden. Er kann von Beauftragten unterstützt werden.

9.2. Der Whistleblower-Referent stellt die vertrauliche Behandlung der Hinweise unter den in Abschnitt 6 dieses Verfahrens vorgesehenen Bedingungen sicher und gewährleistet die Vertraulichkeit, den Schutz und die Aufbewahrungsfrist der im Zusammenhang mit der Bearbeitung des Hinweises erhobenen personenbezogenen Daten unter den in Abschnitt 8 dieses Verfahrens vorgesehenen Bedingungen. Dasselbe gilt für seine Beauftragten.

9.3. Der Whistleblower-Referent kann bei der Bearbeitung von Hinweisen auf interne oder externe Sachverständige zurückgreifen und ganz allgemein die verschiedenen Abteilungen der Organisation in Anspruch nehmen.

9.4. Die Organisation stellt sicher, dass jeder Dienstleister, der mit der Verwaltung dieses Systems ganz oder teilweise beauftragt werden kann, sich zu Vertraulichkeit der Daten verpflichtet, und alle manuellen oder computergestützten personenbezogenen Datenträger am Ende seiner Beauftragung vernichten oder zurückgeben.[8]

9.5. Nach Überprüfung eines Hinweises formuliert der Referent gegebenenfalls Empfehlungen an die Personalabteilung bezüglich möglicher Disziplinarmaßnahmen gegen die von dem Hinweis betroffenen Personen oder den Hinweisgeber im Falle eines bösgläubigen Hinweises oder einer Meldung an die zuständigen Behörden. Die Formulierung, die zur Beschreibung der Sachverhalten verwendet wird, weist auf deren mutmaßliche Natur hin.

9.6. Abweichend vom Vorstehenden macht der Whistleblower-Referent den Geschäftsführer und/oder den Compliance-Ausschuss unverzüglich auf Situationen, Behauptungen oder Berichte aufmerksam, von denen er weiß, dass:

[8] Jede Übermittlung personenbezogener Daten außerhalb der Europäischen Union an eine juristische Person mit Sitz in einem Land, das nicht Mitglied der Europäischen Union ist und keinen ausreichenden Schutz im Sinne von Artikel 68 des Gesetzes vom 6. Januar 1978 in seiner geänderten Fassung bietet, erfolgt in Übereinstimmung mit den besonderen Bestimmungen des Gesetzes Nr. 78-17 vom 6. Januar 1978 in seiner geänderten Fassung über internationale Datenübermittlungen und der Datenschutz-Grundverordnung (Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016).

9.6.1. ein Geschäftsführer einer der Tochtergesellschaften, ein Mitglied des Exekutivausschusses oder des Verwaltungsrates beschuldigt wird, im Sinne der ordentlichen Unternehmensführung; oder

9.6.2. ein Verdacht oder ein Hinweis auf Geldwäsche, private oder öffentliche Korruption, Bestechung, internen oder externen Betrug oder schwere Verletzung (oder Gefahr einer Verletzung) der Menschenrechte und Grundfreiheiten besteht.

## 10. NACHBEARBEITUNG DES HINWEISE

10.1. Um die Wirksamkeit des Whistleblower-Systems beurteilen zu können, kann der Whistleblower-Referent ein jährliches statistisches Monitoring der Entgegennahme, der Bearbeitung und der Weiterverfolgung von Whistleblower-Hinweisen einrichten.

10.2. Diese jährlichen statistischen Monitorings kann die Anzahl der eingegangenen Hinweise, der abgeschlossenen Fälle, der Fälle, die Anlass zu einer Untersuchung gegeben haben oder geben, die Anzahl und die Art der Maßnahmen, die während und am Ende der Untersuchung ergriffen wurden (Vorsichtsmaßnahmen, Einleitung von Disziplinar- oder Gerichtsverfahren, verhängte Sanktionen usw.), aufzeigen.

## 11. VERTEILUNG

11.1. Die Organisation wird ihre Belegschaft und Mitarbeiter auf die Existenz ihres Whistleblowing-Rechts aufmerksam machen, z. B. durch Plakate oder Benachrichtigungen.

## 12. KONTAKT

12.1. Bei Fragen zu diesem Verfahren und zu den Garantien, die das Whistleblowing-Recht regeln, wenden sich Mitarbeiter innerhalb oder außerhalb der Organisation an:

12.1.1. complianceofficer@circet.com

12.2. Anfragen bezüglich des Whistleblowing-Rechts gelten nicht als Hinweis, die in den Anwendungsbereich dieses Verfahrens fällt.

# 5. PROCEDURE MET BETREKKING TOT KLOKKENLUIDERS

## 1. OVERZICHT

1.1. Werknemers en externe of losse medewerkers van de Circet-groep (‘de organisatie') kunnen vertrouwelijk melding doen van elke ernstige inbreuk op het algemene belang en de bepalingen in de Gedragscode. Voor het goed functioneren van de organisatie moeten zij de organisatie op de hoogte kunnen stellen van een mogelijke of bewezen inbreuk op wet- en regelgeving en op de interne procedures.

1.2. De hierna beschreven procedure (de 'procedure’) biedt personen die dat willen de mogelijkheid hun recht van melding uit te oefenen en gebruik te maken van de klokkenluidersbescherming waarin de Franse wet nr. 2016-1691 van 9 december 2016 met betrekking tot transparantie, corruptiebestrijding en modernisering van de economie, en de bepalingen van het Franse besluit nr. 2017-564 van 19 april 2017 voorzien.

1.3. Deze procedure is facultatief en de organisatie neemt geen maatregelen tegen personen die er geen gebruik van maken. De procedure is niet bedoeld als vervanging van de normale wegen voor interne communicatie via de hiërarchische structuur van de organisatie of met de direct of indirect leidinggevende, de hr-afdeling of een vertegenwoordiger van werknemers of personeel: de procedure is dus een aanvulling.

1.4. De organisatie heeft speciale voorzorgsmaatregelen getroffen om een kader te bieden voor de behandeling van die meldingen, conform toepasselijke wet- en regelgeving, met inbegrip van het besluit (Délibération) nr 2017-191 van 22 juni 2017 ter vervanging van besluit (Délibération) nr 2005-305 van 8 december 2005 over de eenmalige toestemming voor de automatische verwerking van persoonsgegevens geïmplementeerd in het kader van een klokkenluidersprocedure op de werkvloer (AU-004) van de CNIL (Commission Nationale Informatique et Liberté) en in navolging van de databeschermingsimpactanalyse uitgevoerd door de Organisatie in uitvoering van het besluit (Délibération) nr 2018-327.

## 2. MELDINGSRECHT

2.1. Het meldingsrecht kan worden samengevat als de mogelijkheid die iedere persoon wordt aangeboden om al dan niet melding te maken can een ernstige inbreuk op het algemene belang die hij of zij zelf heeft waargenomen.

2.2. De melding kan betrekking hebben op een misdrijf of overtreding, een ernstige en duidelijke schending van een regel, wet of internationaal verdrag dat Frankrijk heeft ondertekend of een ernstige dreiging voor of schending van het algemene belang[9].

[9] Feiten, gegevens of documenten, in welke vorm of op welke drager dan ook, die onder de geheimhouding van de nationale defensie, het medisch geheim of het ambtsgeheim tussen advocaat en zijn cliënt vallen, zijn uitgesloten van het meldingssysteem dat in deze procedure wordt beschreven.

2.3. De melding kan bijvoorbeeld betrekking hebben op een feit of gedrag waarmee wet- en regelgeving wordt overtreden.

2.4. Ook situaties die niet lijken te voldoen aan de bepalingen van de Gedragscode van de organisatie kunnen worden gemeld

## 3. DE KLOKKENLUIDER

3.1. Alle interne medewerkers (voltijdse of deeltijdse werknemers, tijdelijke werknemers, leercontracten en stagiairs) en externe of losse medewerkers (inclusief onderaannemers en leveranciers) van de organisatie kunnen een melding doen. Personen die deelnemen aan activiteiten die verband houden met de organisatie maar niet door de organisatie worden georganiseerd, kunnen hun melding doen bij de organisator van die activiteit.

3.2. Een melding kan alleen worden gedaan door:
(a) een natuurlijke persoon, die
(b) te goeder trouw handelt,
(c) zelf geen belang heeft bij de melding,
(d) de betreffende feiten zelf heeft geconstateerd en
(e) daarbij de procedure volgt zoals beschreven in Sectie 4.

3.2.1. De melding moet te goeder trouw worden gedaan, dus vanuit de redelijke overtuiging dat de feiten waar zijn op het moment van melding.

3.2.2. De melding moet belangeloos zijn, dus de melder maakt geen aanspraak op een beloning, een voordeel of een tegenprestatie en handelt niet met de bedoeling om iemand schade te berokkenen.

3.2.3. Ten slotte moet de klokkenluider uit eigen waarneming kennis hebben gekregen van de feiten die hij/zij meldt. Een melding van feiten die de klokkenluider niet zelf heeft geconstateerd, maar van horen zeggen heeft of die zijn gebaseerd op een vermoeden of een niet onderbouwde bewering, wordt als onontvankelijk beschouwd.

## 4. EEN MELDING DOEN

4.1. Interne werknemers van de organisatie kunnen hun vaststellingen direct melden bij de door de organisatie aangewezen personen (de ‘vertrouwenspersonen') en via het online toegankelijke meldingsplatform.

Zoals eerder vermeld is de procedure een aanvulling en geen vervanging van de normale interne communicatiekanalen die via de hiërarchische structuur van de organisatie lopen. Er wordt aangeraden om eerst contact op te nemen met de direct of indirect leidinggevende, de hr-afdeling of een personeels- of managementvertegenwoordiger.

4.2. Externe medewerkers van de organisatie kunnen een melding doen bij de vertrouwenspersoon en via ons online toegankelijke meldingsplatform.

4.3. De melding moet alle feitelijke informatie of relevante documenten bevatten die de melding kunnen onderbouwen. De melding moet zo volledig, nauwkeurig, gedetailleerd en gedocumenteerd mogelijk zijn: de melding moet met name de datum bevatten waarop de feiten plaatsvonden alsook de identiteit van de betrokken personen indien de klokkenluider over deze informatie beschikt.

4.4. De klokkenluider moet uitleggen hoe hi/zij persoonlijk op de hoogte is gekomen van de feiten en of er een derde partij van die feiten op de hoogte is gesteld door de klokkenluider zelf of op een andere manier.

4.5. De klokkenluider wordt gevraagd om alle informatie te verstrekken zodat de organisatie, met respect voor de vertrouwelijkheid van zijn of haar identiteit, contact met hem/haar kan opnemen (naam, voornaam, contactmethode) en de melding kan bespreken.

4.6. Bij uitzondering kan een anonieme melding in behandeling worden genomen wanneer de ernst van de genoemde feiten duidelijk is en de feiten voldoende gedetailleerd zijn. De behandeling van anonieme meldingen is onderworpen aan speciale voorzorgsmaatregelen, zoals een voorafgaand onderzoek door de eerste persoon aan wie de melding werd gedaan en de bepaling of de melding moet worden verspreid onder betrokkenen via het meldingsinstrument. De beveiligde internetpagina van het speciale platform maakt anonimiteit mogelijk, maar moedigt die niet aan. Het is moeilijker en soms zelfs onmogelijk om een anonieme melding te behandelen en vast te stellen of ze gegrond is. De organisatie adviseert dan ook een melding met naam te doen. Het onderzoek is gemakkelijker wanneer de identiteit van de klokkenluider bekend is, omdat dan met hem of haar kan worden overlegd. De organisatie stelt alles in het werk om geheimhouding te garanderen.

## 5. VERTROUWELIJKHEID

5.1. De organisatie garandeert de strikte vertrouwelijkheid van:
- 5.1.1. de identiteit van de klokkenluider,
- 5.1.2. de identiteit van de personen op wie de melding betrekking heeft,
- 5.1.3. alle informatie die werd ontvangen binnen het kader van de behandeling van de melding.

5.2. Na ontvangst van de melding communiceren de vertrouwenspersoon (en/of eventuele gemachtigden) en de klokkenluider via het meldingsplatform. Wanneer de klokkenluider geen toegang tot dit platform heeft en een ander communicatiemiddel gebruikt, is dat niet van invloed op de eventuele ontvankelijkheid van de melding en stelt dat de klokkenluider niet bloot aan sancties. Toegang tot het meldingsplatform is voorbehouden aan de vertrouwenspersoon en eventuele gemachtigden.

5.3. Bij melding per post wordt geadviseerd met een dubbele envelop te werken: alle informatie voor de melding wordt in een envelop gedaan, de ‘binnenenvelop’, en die envelop wordt gesloten in een tweede envelop gedaan.

## 6. ONDERZOEK VAN DE MELDINGEN

6.1. De melding wordt door de organisatie zo snel mogelijk gecontroleerd, behandeld en geanalyseerd met respect voor het vertrouwelijke karakter van de melding. De klokkenluider wordt niet gevraagd zelf onderzoek te doen en ook niet om de juridische kwalificatie van de gemelde feiten vast te stellen.

6.2. De klokkenluider krijgt onmiddellijk via het platform een verzendbevestiging van de melding, met een geheime code die hij/zij moet bewaren. De verzendbevestiging betekent niet automatisch dat de melding ontvankelijk is.

6.3. Het onderzoek naar de ontvankelijkheid van de melding gebeurt binnen een redelijke termijn: in principe binnen maximaal 15 werkdagen na ontvangst van de melding. De klokkenluider wordt op de hoogte gesteld van de ontvankelijkheid. Als de melding ontvankelijk is, wordt er een onderzoek gedaan naar de waarheid van de gemelde feiten.

6.3.1. De tijd die daarvoor nodig is, kan variëren afhankelijk van de elementen van de melding.

6.4. Als de klokkenluider na een redelijke termijn na de melding nog niet op de hoogte is gesteld van de ontvankelijkheid, kan die de melding doen bij de rechterlijke instanties (bijvoorbeeld een officier van justitie of rechter) of een administratieve instantie (zoals de prefect, de Commission Nationale de l'Informatique et des Libertés (CNIL) of het Agence Française Anticorruption (AFA)). Wanneer de melding binnen drie maanden door geen van die instanties is behandeld, kan de klokkenluider als ultieme optie de kwestie openbaar melden (bijvoorbeeld via de media, een vereniging, een ngo of een vakbond).

6.5. Alleen bij een groot en dreigend gevaar of bij een risico van onherstelbare schade kan de melding rechtstreeks aan de bevoegde instanties worden gedaan of openbaar worden gemaakt.

6.5.1. Onder een groot en dreigend gevaar verstaan we elk soort gevaar waarbij doden of gewonden kunnen vallen binnen een afzienbare termijn.

6.6. Bij twijfel kan iedereen de kwestie melden bij de ombudsman en zich laten adviseren over de instantie waar de melding moet worden gedaan. Een melding bij die ombudsman moet schriftelijk worden gedaan volgens het dubbele-envelopsysteem. Alle elementen van de aanhangigmaking moeten in een envelop, de binnenenvelop, worden gedaan, die gesloten in een tweede envelop, de buitenenvelop, aan de ombudsman wordt gericht. Op de binnenenvelop moet alleen staan: ‘MELDING IN HET KADER VAN DE WET VAN 9 DECEMBER 2016 GEDAAN OP (verzenddatum).’ Op de buitenenvelop komt het adres: Défenseur des droits, Libre réponse 71120, 75342 PARIS CEDEX 07**.**

## 7. BESCHERMING TEGEN REPRESAILLES

7.1. De organisatie beschermt ieder die belangeloos en te goeder trouw feiten meldt die wijzen op een overtreding of misdrijf, ook als de gesignaleerde feiten achteraf onjuist blijken of geen reden voor vervolging geven.

7.2. Geen enkele persoon kan worden uitgesloten van een wervingsprocedure of toegang tot een stage of een opleiding. Evenmin kan een werknemer gesanctioneerd of ontslagen worden of nadeel ondervinden van een direct of indirect discriminerende maatregel, met name op het gebied van beloning, winstdeelname of toekenning van aandelen, scholing, herinzetting, benoeming, kwalificatie, classificatie, promotie, overplaatsing of contractverlenging.

7.3. Elke werknemer of medewerker die meent slachtoffer te zijn van represailles voor het te goeder trouw melden van of getuigen over feiten die een overtreding of misdrijf vormen waarvan hij/zij tijdens de taakuitoefening kennis heeft gekregen, kan dat melden aan de vertrouwenspersoon of, in geval van ontslag, voorleggen aan de rechter.

7.4. Misbruik van het meldingsinstrument, met name in de vorm van een valse melding (melding van gegevens waarvan de melder weet dat ze deels of gedeeltelijk onjuist zijn) of een melding te kwader trouw leidt tot vervolging van de melder conform de wet (artikel 226-10 van de Franse strafwet) en, conform het interne reglement, tot disciplinaire maatregelen.

7.5. Elke werknemer die de indiening van een melding belemmert of heeft belemmerd, of die represailles tegen de klokkenluider heeft ondernomen, wordt gerechtelijk vervolgd en kan, conform het interne reglement, onderworpen worden aan disciplinaire maatregelen.

## 8. VERWERKING VAN PERSOONSGEGEVENS

8.1. De organisatie registreert in verband met de behandeling van een melding alleen de volgende gegevens:

- 8.1.1. identiteit, functie en gegevens van de klokkenluider;
- 8.1.2. identiteit, functie en gegevens van de personen op wie de melding betrekking heeft;
- 8.1.3. identiteit, functie en gegevens van de personen die betrokken zijn bij de ontvangst of de behandeling van de melding;
- 8.1.4. de gesignaleerde feiten;
- 8.1.5. gegevens/documenten die zijn ontvangen binnen het kader van de controle van de gesignaleerde feiten;
- 8.1.6. verslag van de controleactiviteiten;
- 8.1.7. resultaten van de melding.

De verzameling en verwerking van deze persoonsgegevens zijn bedoeld om de ontvankelijkheid van de melding te bepalen, de feiten te controleren en zo nodig de juiste corrigerende maatregelen te treffen. Ze stellen de organisatie in staat aan haar juridische verplichtingen te voldoen (met name voortvloeiend uit de Franse 'Wet Sapin II' van 9 december 2016 en de Franse wet van 27 maart 2017 met betrekking tot de plicht tot waakzaamheid) en om haar legitieme belangen te beschermen (door handhaving van de wet en de ethische principes van de organisatie).

8.2. Ieder kan zijn of haar recht op toegang, correctie en verzet tegen het gebruik van de gegevens binnen het wettelijke en reglementaire kader uitoefenen door contact op te nemen met de betreffende vertrouwenspersoon.

8.3. In geen enkel geval kan de persoon op wie een melding betrekking heeft informatie krijgen over de identiteit van de klokkenluider via de persoon die de melding analyseert.

8.4. De melder en de persoon op wie de melding van toepassing is, kunnen zich laten bijstaan door een persoon van eigen keuze uit de organisatie, in alle stadia van het proces.

8.5. Elk gegeven met betrekking tot een melding waarvan wordt geoordeeld dat die buiten het bereik van de onderhavige procedure valt, wordt verwijderd of geanonimiseerd en gearchiveerd door de organisatie.

8.6. Als een melding verder niet in behandeling wordt genomen, zal de organisatie alle elementen van het meldingsdossier die te herleiden zijn naar de melder en de personen waarop de melding betrekking had verwijderen. Die gegevens worden uiterlijk drie maanden na de afsluiting van de acties voor de bepaling van de ontvankelijkheid of de controle van de melding verwijderd.

8.7. Wanneer er een disciplinaire procedure wordt gestart of vervolging wordt ingesteld op een of meer personen op wie de melding betrekking heeft, worden de gegevens met betrekking tot de melding bewaard tot het eind van de procedure.

## 9. VERTROUWENSPERSONEN

9.1. De vertrouwenspersoon ontvangt en analyseert de meldingen die hem of haar bereiken via willekeurig welk middel, met name via de beveiligde website, gewone post, e-mail, telefoon of in persona. Hij/zij kan zich laten bijstaan door anderen.

9.2. De vertrouwenspersoon waarborgt de vertrouwelijke behandeling van de meldingen volgens de bepalingen in Sectie 6 van deze procedure. Hij/zij is verantwoordelijk voor de vertrouwelijkheid, bescherming en bewaartermijn van de persoonsgegevens die in verband met de behandeling van de melding werden ontvangen conform de bepalingen in Sectie 8 van deze procedure. Dat geldt ook voor zijn of haar gemachtigden.

9.3. De vertrouwenspersoon kan interne of externe deskundigen inschakelen voor de behandeling van meldingen en, meer in het algemeen, gebruikmaken van verschillende diensten van de organisatie.

9.4. De organisatie zorgt ervoor dat de dienstverlener die wordt aangewezen voor het gehele of gedeeltelijke beheer van dit meldingsinstrument de gegevens niet voor andere doeleinden gebruikt, de vertrouwelijkheid ervan waarborgt, de maximale bewaartermijn respecteert en overgaat tot vernietiging of teruggave van alle materiële of digitale persoonlijke gegevensdragers aan het eind van de procedure.[10]

9.5. Na afloop van het onderzoek van een melding formuleert de vertrouwenspersoon, indien van toepassing, aanbevelingen voor de hr-afdeling voor eventuele disciplinaire maatregelen voor de personen op wie de melding van toepassing is of voor de klokkenluider indien die te kwader trouw heeft gehandeld. Ook kan de vertrouwenspersoon uiteindelijk melding doen aan de bevoegde autoriteiten. De gebruikte formuleringen voor de beschrijving van de aard van de gesignaleerde feiten geven hun vermeende karakter aan.

[10]Elke overdracht van persoonsgegevens buiten de Europese Unie naar een rechtspersoon in een land buiten de Europese Unie en die niet voldoende beveiliging biedt in de zin van artikel 68 van de Franse gewijzigde wet van 6 januari 1978, wordt uitgevoerd conform de specifieke bepalingen van de Franse gewijzigde wet nr. 78-17 van 6 januari 1978 met betrekking tot internationale gegevensoverdrachten en van de

9.6. In uitzondering op het voorgaande stelt de vertrouwenspersoon onverwijld de algemeen directeur en/of de compliance-commissie op de hoogte van situaties, beschuldigingen of meldingen waarvan hij/zij kennis heeft:

9.6.1. wanneer het gaat om een algemeen directeur van een dochteronderneming, een lid van het uitvoerend comité of de raad van bestuur, conform het principe van goed bestuur; of

9.6.2. in het geval van een vermoeden of beschuldiging van witwassen, omkoping van een privépersoon of ambtenaar, beïnvloedingspraktijken, interne of externe fraude of een ernstig gevaar (of dreiging van gevaar) voor de mensenrechten en fundamentele vrijheden.

## 10. OPVOLGING VAN MELDINGEN

10.1. Om de effectiviteit van het meldingsinstrument te beoordelen kan de vertrouwenspersoon een jaarlijkse statistische analyse instellen met betrekking tot de ontvangst, de verwerking en het vervolg van meldingen.

10.2. Die statistische jaaranalyse kan laten zien hoeveel meldingen er zijn binnengekomen, hoeveel dossiers zijn gesloten, hoeveel dossiers aanleiding waren of zijn voor een onderzoek, hoeveel en welke maatregelen zijn genomen tijdens en na het onderzoek (zoals maatregelen om bewijsmateriaal te beschermen, in gang zetten van disciplinaire of strafrechtelijke procedures, opgelegde sancties enz.).

## 11. VERSPREIDING

11.1. De organisatie stelt haar werknemers en medewerkers in kennis van hun meldingsrecht, onder meer met bijvoorbeeld affiches of via directe interne communicatie.

## 12. CONTACT

12.1. Voor vragen over deze procedure en de garanties rond het meldingsrecht omlijsten, kunnen interne en externe medewerkers van de organisatie contact opnemen met:

12.1.1. complianceofficer@circet.com

12.2. Verzoeken om informatie met betrekking tot het meldingsrecht worden niet beschouwd als een melding binnen het kader van deze procedure.

# 6. PROCEDURA PER I SEGNALATORI DI ILLECITI

## 1. SINTESI

I dipendenti e i collaboratori esterni od occasionali del Gruppo CIRCET ("l'Organizzazione") possono segnalare, in maniera riservata, eventuali gravi violazioni dell'interesse generale e delle disposizioni del Codice di condotta. Il corretto funzionamento dell'organizzazione fa sì che questi possano informare chi di dovere del mancato rispetto (potenziale o effettivo) delle disposizioni legali e regolamentari, nonché delle procedure interne.

La procedura descritta di seguito (la "Procedura") consente a coloro che lo desiderano di esercitare il proprio diritto di segnalazione e beneficiare della protezione dei segnalatori di illeciti prevista dalla legge francese n. 2016-1691 del 9 dicembre 2016 relativa alla trasparenza, alla lotta contro la corruzione e alla modernizzazione della vita economica e secondo le modalità di cui al decreto francese n. 2017-564 del 19 aprile 2017.

Questa Procedura è facoltativa e l'organizzazione non intraprenderà alcuna azione nei confronti di coloro che decidono di non avvalersene. Essa non intende sostituire i normali canali di comunicazione interna attraverso la struttura gerarchica dell'organizzazione e con il superiore gerarchico, diretto o indiretto, il reparto risorse umane o un rappresentante dei dipendenti o del personale, ed ha pertanto un carattere sussidiario.

L'organizzazione prevede precauzioni particolari per inquadrare la gestione di tali segnalazioni, in conformità alle leggi e ai regolamenti applicabili, tra cui la delibera n. 2017-191 del 22 giugno 2017 che modifica la delibera n. 2005-305 dell'8 dicembre 2005 relativa all'autorizzazione unica al trattamento automatizzato dei dati personali attuata nell'ambito dei sistemi di segnalazione professionale (AU-004) della CNIL (Commissione nazionale per l'informatica e le libertà) e in seguito alla valutazione d'impatto sulla protezione dei dati (AIPD) effettuata dall'organizzazione in applicazione della delibera n. 2018-327 della CNIL.

## 2. IL DIRITTO DI SEGNALAZIONE

2.1. Il diritto di segnalazione può essere sintetizzato come la facoltà offerta a qualsiasi persona di decidere o meno di denunciare una grave violazione dell'interesse generale di cui è personalmente a conoscenza.

2.2. La segnalazione può riguardare qualunque reato o delitto, qualunque violazione grave e manifesta di un regolamento, di una legge o di un trattato internazionale ratificato dalla Francia, o infine qualunque minaccia o grave pregiudizio per l'interesse generale[11].

[11] I fatti, le informazioni e i documenti, indipendentemente dalla forma o dal supporto, coperti dal segreto della difesa nazionale, dal segreto medico o dal segreto della relazione tra un avvocato e il suo cliente sono esclusi dal regime di segnalazione definito nella presente Procedura.

2.3. Ad esempio, la segnalazione può riguardare qualsiasi fatto o comportamento che violi le regole contenute in leggi e regolamenti.

2.4. Può essere oggetto di segnalazione anche qualsiasi situazione che non sembri conforme alle disposizioni del codice di condotta dell'organizzazione.

## 3. IL SEGNALATORE DI ILLECITI

3.1. Tutti i collaboratori interni (dipendenti a tempo pieno o parziale, temporanei, apprendisti e tirocinanti) e i collaboratori esterni od occasionali (compresi subappaltatori o fornitori) dell'organizzazione possono segnalare un illecito. Le persone che partecipano ad attività che sono legate all'organizzazione ma non fanno capo alla stessa, sono invitate a indirizzare eventuali segnalazioni all'organizzatore dell'attività.

3.2. Per avviare una segnalazione è necessario:
(a) essere una persona fisica;
(b) agire in buona fede;
(c) agire in maniera disinteressata;
(d) segnalare fatti di cui si è personalmente a conoscenza;
(e) attenersi alla Procedura descritta nella Sezione 4.

3.2.1. La segnalazione deve avere luogo in buona fede, ovvero sulla base di una ragionevole convinzione che i fatti siano veritieri al momento della segnalazione.

3.2.2. La segnalazione deve essere disinteressata, ossia l'autore non deve pretendere alcun compenso, vantaggio o contropartita, e non deve agire con l'intento di nuocere ad altri.

3.2.3. Infine, il segnalatore di illeciti deve essere venuto a conoscenza personalmente dei fatti che riferisce. La segnalazione di fatti di cui l'autore non è direttamente a conoscenza e che sono stati riferiti da una terza persona, o basati su sospetti o accuse non documentate, sarà considerata inammissibile.

## 4. SEGNALARE UN ILLECITO

4.1. I collaboratori interni dell'organizzazione possono inoltrare eventuali segnalazioni direttamente ai referenti appositamente designati dall'organizzazione per la ricezione e la valutazione delle segnalazioni (i "Referenti per le segnalazioni"), nonché tramite la nostra piattaforma di segnalazione accessibile online.

Si ricorda che questa procedura ha carattere sussidiario e non intende sostituire i normali canali di comunicazione interna attraverso la struttura gerarchica dell'organizzazione, come il superiore gerarchico, diretto o indiretto, il reparto risorse umane o un rappresentante dei dipendenti o del personale, di cui i collaboratori interni sono invitati ad avvalersi.

4.2. I collaboratori esterni all'organizzazione possono trasmettere eventuali segnalazioni al Referente per le segnalazioni, nonché tramite la nostra piattaforma di segnalazione accessibile online.

4.3. Occorre indicare tutti i fatti, le informazioni o i documenti pertinenti a sostegno della denuncia, in modo che la segnalazione sia quanto più completa, accurata, dettagliata e documentata possibile in particolare, la segnalazione deve indicare la data in cui si sono verificati i fatti e l'identità delle persone coinvolte, quando tali elementi sono noti al segnalatore.

4.4. L'autore deve precisare i motivi per cui è venuto personalmente a conoscenza dei fatti e l'eventule divulgazione dei fatti a terzi, ad opera del segnalatore stesso o in altro modo.

4.5. L'autore della segnalazione è invitato a fornire tutti gli elementi che consentano all'organizzazione di contattarlo (cognome, nome, modalità di contatto) e di comunicare in merito alla segnalazione, pur preservando la riservatezza della sua identità.

4.6. In via eccezionale, potranno essere prese in considerazione segnalazioni anonime, a condizione che sia accertata la gravità dei fatti citati e che tali fatti siano sufficientemente dettagliati. La gestione delle segnalazioni di questo tipo sarà accompagnata da precauzioni specifiche, ad esempio un esame preliminare da parte del primo destinatario ma anche la valutazione dell'opportunità che esse vengano diffuse nell'ambito del meccanismo di segnalazione. Il sito web protetto della piattaforma dedicata consente l'anonimato ma non lo incoraggia. È più difficile e talvolta impossibile gestire una segnalazione anonima o accertare la fondatezza dei fatti. L'organizzazione raccomanda che la segnalazione sia nominativa; il processo di indagine è infatti facilitato quando l'identità dell'autore è nota, in modo da poter instaurare un dialogo, fermo restando che l'organizzazione si impegna a garantirne la riservatezza.

## 5. RISERVATEZZA

5.1. L'organizzazione garantisce la rigorosa riservatezza:
5.1.1. dell'identità dell'autore di una segnalazione;
5.1.2. dell'identità delle persone oggetto della segnalazione;
5.1.3. di tutte le informazioni raccolte nell'ambito dell'elaborazione della segnalazione.

5.2. Una volta ricevuta la segnalazione, gli scambi tra il Referente per le segnalazioni (e/o eventuali delegati) e l'autore hanno luogo tramite la piattaforma di segnalazione. Il mancato utilizzo di questo sistema di messaggistica ovvero l'utilizzo di altri mezzi di comunicazione non compromettono l'eventuale ammissibilità della segnalazione, né espongono l'autore a sanzioni. L'accesso al sistema di messaggistica della piattaforma è riservato ai Referenti per le segnalazioni e a eventuali delegati.

5.3. In caso di segnalazione tramite posta, si consiglia di utilizzare il metodo della doppia busta: tutti gli elementi della segnalazione vengono inseriti in una busta chiusa, detta busta interna, che verrà a sua volta inserita in una seconda busta.

## 6. ELABORAZIONE DELLE SEGNALAZIONI

6.1. La verifica, l'elaborazione e l'analisi delle segnalazioni vengono effettuate dall'organizzazione al più presto possibile e nel rispetto del carattere confidenziale della situazione. L'autore della segnalazione non è invitato a indagare in prima persona, né a cercare di stabilire l'inquadramento giuridico dei fatti segnalati.

6.2. L'autore riceverà immediatamente, attraverso la piattaforma, una conferma di trasmissione della segnalazione e dovrà conservare il proprio codice riservato. La conferma di avvenuta trasmissione non costituisce un'attestazione circa l'ammissibilità della segnalazione.

6.3. L'esame dell'ammissibilità della segnalazione ha luogo entro un termine ragionevole, generalmente non superiore a 15 giorni lavorativi, dopo la ricezione della stessa. L'autore viene informato dell'esito circa l'ammissibilità. Se la segnalazione è ammissibile, verrà condotta un'indagine per determinare la fondatezza dei fatti riferiti.
6.3.1. Tuttavia, i tempi possono variare a seconda delle caratteristiche della segnalazione.

6.4. Se, trascorso un ragionevole periodo di tempo dalla segnalazione, l'autore non è stato informato circa la sua ammissibilità, potrà inoltrarla alle autorità giudiziarie (ad es. procuratore o giudice) o amministrative (ad es. prefetto, Commissione nazionale per l'informatica e le libertà - CNIL, Agenzia francese anticorruzione - AFA). In ultima istanza, e in assenza di presa in carico da parte di una di queste autorità entro tre mesi, l'autore potrà renderla pubblica (ad es. divulgazione ai media, ad un'associazione, una ONG o un sindacato).

6.5. La segnalazione può essere portata direttamente a conoscenza delle autorità competenti o resa pubblica solo in caso di pericolo grave e imminente o in presenza di un rischio di danno irreversibile.

6.5.1. Con pericolo grave e imminente si intende qualunque tipo di rischio capace di provocare lesioni o la morte e la cui materializzazione sia vicina nel tempo.

6.6. In caso di dubbio, qualsiasi persona può trasmettere la propria segnalazione al *Défenseur des droits* in modo che venga indirizzata all'organismo più idoneo a riceverla. L'invio della segnalazione al *Défenseur des droits* deve avere luogo tramite posta, per iscritto e in busta doppia. Tutti gli elementi della segnalazione devono essere inseriti in una busta chiusa, detta busta interna, che verrà inserita in una seconda busta indirizzata al *Défenseur des droits*, detta busta esterna. Sulla busta interna dovrà figurare solo quanto segue: "INVIO DI UNA SEGNALAZIONE AI SENSI DELLA LEGGE DEL 9 DICEMBRE 2016 EFFETTUATO IL (data dell'invio)." Sulla busta esterna sarà riportato l'indirizzo: Défenseur des droits, Libre réponse 71120, 75342 PARIGI CEDEX 07 - FRANCIA**.**

## 7. PROTEZIONE CONTRO LE RAPPRESAGLIE

7.1. L'organizzazione protegge chiunque porti alla sua attenzione, in maniera disinteressata e in buona fede, fatti che costituiscono un reato o un delitto, anche qualora i fatti si rivelassero inesatti o non dessero luogo ad alcuna azione.

7.2. Nessun individuo può essere escluso da una procedura di assunzione o dall'accesso a un tirocinio o periodo di formazione e nessun dipendente può essere sanzionato, licenziato o sottoposto a misure discriminatorie, dirette o indirette, anche in materia di retribuzione, misure di interessenza o distribuzione di azioni, formazione, reinserimento, assegnazione, qualificazione, classificazione, promozione professionale, trasferimento o rinnovo di contratto.

7.3. Qualsiasi dipendente o collaboratore che ritenga di essere stato oggetto di ritorsioni per aver segnalato o testimoniato, in buona fede, fatti che costituiscono un reato o un delitto e di cui è venuto a conoscenza nell'esercizio delle proprie funzioni, può segnalarlo al Referente per le segnalazioni oppure rivolgersi al tribunale del lavoro con procedura d'urgenza in caso di licenziamento.

7.4. Qualsiasi uso improprio del meccanismo, sotto forma, ad esempio, di segnalazione diffamatoria (segnalazione di informazioni che l'autore sa essere totalmente o parzialmente inesatte) o in malafede, espone l'autore alle azioni giudiziarie previste dalla legge (articolo 226-10 del Codice penale francese) e, in conformità al Regolamento interno, ad azioni disciplinari.

7.5. Qualsiasi dipendente che intralci o abbia intralciato la trasmissione di una segnalazione o che abbia adottato misure ritorsive nei confronti dell'autore di una segnalazione va incontro ad azioni giudiziarie e può, in conformità al Regolamento interno, essere soggetto ad azioni disciplinari.

## 8. TRATTAMENTO DEI DATI PERSONALI

8.1. Ai fini dell'elaborazione di una segnalazione, l'organizzazione si limita a registrare i seguenti dati:

8.1.1. identità, funzioni e informazioni di contatto dell'autore;

8.1.2. identità, funzioni e informazioni di contatto delle persone oggetto della segnalazione;

8.1.3. identità, funzioni e informazioni di contatto delle persone coinvolte nella ricezione o nell'elaborazione della segnalazione;

8.1.4. i fatti segnalati;

8.1.5. gli elementi raccolti in fase di accertamento dei fatti segnalati;

8.1.6. resoconto delle operazioni di accertamento;

8.1.7. azioni adottate a seguito della segnalazione.

Lo scopo della raccolta e del trattamento di tali dati personali è quello di determinare l'ammissibilità delle segnalazioni, accertare i fatti e adottare, se necessario, le opportune misure correttive. Essi consentono quindi all'organizzazione di rispettare i propri obblighi legali (derivanti in particolare dalla cosiddetta legge "Sapin II" del 9 dicembre 2016 e dalla legge del 27 marzo 2017 sul dovere di vigilanza) e di tutelare i propri legittimi interessi (nel rispetto della legge e dei principi etici dell'organizzazione).

8.2. Il diritto di accesso, rettifica e opposizione all'uso dei dati può essere esercitato, a livello giuridico e normativo, contattando il Referente per le segnalazioni all'indirizzo fornito.

8.3. In nessun caso la persona oggetto di segnalazione può ottenere dal responsabile del trattamento informazioni sull'identità dell'autore della segnalazione.

8.4. Il mittente di una segnalazione o la persona oggetto della stessa possono farsi assistere da qualsiasi persona di loro scelta appartenente all'organizzazione e in tutte le fasi della procedura.

8.5. Tutti i dati relativi a una segnalazione che non vengano considerati rientranti nel campo di applicazione del meccanismo della presente procedura saranno eliminati o archiviati dall'organizzazione previa anonimizzazione.

8.6. Qualora una segnalazione non desse luogo ad alcuna azione, l'organizzazione distruggerà tutti gli elementi del relativo fascicolo che permettano di identificarne l'autore e le persone interessate. Tale distruzione dovrà avere luogo entro tre mesi dalla chiusura di tutte le operazioni di ammissibilità o di accertamento della segnalazione.

8.7. Quando vengono avviate procedure disciplinari o azioni legali nei confronti di una o più persone oggetto della segnalazione, i dati relativi a quest'ultima vengono conservati fino al termine della procedura.

## 9. I REFERENTI PER LE SEGNALAZIONI

9.1. Il Referente per le segnalazioni riceve e analizza le segnalazioni trasmesse con qualsiasi mezzo, in particolare attraverso il sito web protetto, tramite posta, posta elettronica, telefono o di persona. Può essere assistito da delegati.

9.2. Il Referente per le segnalazioni assicura il trattamento confidenziale delle segnalazioni alle condizioni stabilite nella Sezione 6 della presente Procedura e garantisce il rispetto della riservatezza, della protezione e della durata di conservazione dei dati personali raccolti nell'ambito del trattamento della segnalazione alle condizioni di cui alla Sezione 8 della presente Procedura. Lo stesso vale per i delegati.

9.3. Il Referente per le segnalazioni può fare ricorso a esperti interni o esterni per la gestione delle segnalazioni e, più in generale, per accedere ai vari servizi dell'organizzazione.

9.4. L'organizzazione si assicura inoltre che il fornitore di servizi eventualmente designato per la gestione, in tutto o in parte, di questo meccanismo si impegni a non utilizzare i dati per scopi impropri, al fine di garantirne la riservatezza, rispettare la durata di conservazione limitata dei dati e procedere alla distruzione o alla restituzione di tutti i supporti fisici o informatici contenenti i dati personali al termine della prestazione.[12]

9.5. Al termine dell'istruzione di una segnalazione, il Referente per le segnalazioni formula, ove opportuno, una serie di raccomandazioni destinate al reparto risorse umane in merito alle eventuali azioni disciplinari da adottare nei confronti dei soggetti coinvolti nella segnalazione ovvero dell'autore, in caso di segnalazione in malafede, o ancora eventuali notifiche alle autorità competenti. Le formulazioni impiegate per descrivere la natura dei fatti segnalati devono indicarne il carattere presunto.

9.6. In deroga a quanto sopra, il Referente per le segnalazioni notifica senza indugio al Direttore generale e/o al comitato per la conformità le situazioni, le accuse o le segnalazioni di cui sia venuto a conoscenza:

9.6.1. che coinvolgano il direttore generale di una delle controllate, un membro del comitato esecutivo o del consiglio di amministrazione, in un'ottica di buona governance; ovvero

9.6.2. riguardanti sospetti o accuse di riciclaggio di denaro, corruzione pubblica o privata, traffico di influenze, frode interna o esterna o grave violazione (o rischio di violazione) dei diritti umani e delle libertà fondamentali.

## 10. MONITORAGGIO DELLE SEGNALAZIONI

10.1. Per poter valutare l'efficacia del meccanismo, il Referente per le segnalazioni può istituire un sistema di monitoraggio statistico annuale sulla ricezione, l'elaborazione e le azioni scaturite in seguito alle segnalazioni.

10.2. Questo monitoraggio statistico annuale può rivelare il numero di segnalazioni ricevute, di fascicoli chiusi e di fascicoli che hanno dato o daranno seguito a un'indagine, il numero e la tipologia di misure adottate durante e al termine delle indagini (misure precauzionali, avvio di procedimenti disciplinari o giudiziari, sanzioni pronunciate, ecc.).

## 11. DISTRIBUZIONE

11.1. L'organizzazione informerà i suoi dipendenti e collaboratori dell'esistenza del loro diritto di segnalazione, anche ad esempio tramite affissione o comunicazione.

## 12. CONTATTI

12.1. Per qualunque domanda relativa alla presente Procedura e alle garanzie relative al diritto di segnalazione, i collaboratori interni o esterni dell'organizzazione sono invitati a contattare:

12.1.1. complianceofficer@circet.com

12.2. Le richieste di informazioni relative al diritto di segnalazione non saranno considerate segnalazioni rientranti nell'ambito del meccanismo di questa Procedura.

[12]Qualsiasi trasferimento di dati personali al di fuori dell'Unione europea ad una persona giuridica stabilita in un paese esterno all'Unione europea che non offra una protezione sufficiente ai sensi dell'articolo 68 della legge francese del 6 gennaio 1978, e successive modifiche, sarà gestito conformemente alle disposizioni specifiche contenute nella legge n. 78-17 del 6 gennaio 1978, e successive modifiche, sui trasferimenti internazionali di dati e nel Regolamento generale sulla protezione dei dati (Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016).