institut ramon llull

PROTOCOLE POUR LA GESTION DU SYSTÈME D'INFORMATION INTERNE

CONSORTIUM DE L'INSTITUT RAMON LLULL

SOMMAIRE

1. CONTEXTE

Le Consortium de l'Institut Ramon Llull (ci-après l'Institut Ramon Llull ou le Consortium) est une entité de droit public à caractère associatif, dotée d'une personnalité juridique propre et sans but lucratif, composée, sur une base volontaire, de l'Administration du Gouvernement de Catalogne, à laquelle elle est rattachée, de l'Administration de la Communauté autonome des Baléares et de la Mairie de Barcelone.

Par l'accord gouvernemental 119/2017, du 1er août, ont été approuvés les nouveaux statuts du Consortium de l'Institut Ramon Llull (DOGC n° 7426 - 3.8.2017), modifiés par l'accord gouvernemental 86/2023, du 11 avril, en raison de l'adhésion de la Mairie de Palma.

En relation avec la mise en œuvre d'un Système d'alertes interne au Consortium de l'Institut Ramon Llull, suite à l'entrée en vigueur de la loi d'État 2/2023 du 20 février, réglementant la protection des personnes qui signalent des infractions réglementaires, ainsi que la lutte contre la corruption (qui transpose la directive [UE] 2019/1937 du Parlement européen et du Conseil, du 23 octobre 2019, relative à la protection des personnes qui signalent des violations du droit de l'UE), et étant donné que l'organisation compte plus de 50 employés, lors de la réunion du Conseil d'Administration du Consortium tenue le 16 juin 2023, conformément aux dispositions de l'article 11, sections e), j) i n) du règlement statutaire, les décisions suivantes ont été adoptées dans le cadre de la mise en œuvre de la loi susmentionnée :

(sic) « Premièrement. — Autoriser l'adhésion au système d'information interne et à la procédure de gestion de l'Administration du Gouvernement de Catalogne, en tant qu'administration rattachée, et ce dans les termes prévus par l'accord gouvernemental, dans le cadre de la loi 2/2023 du 20 février, réglementant la protection des personnes qui signalent des infractions réglementaires, ainsi que la lutte contre la corruption, jusqu'à ce que l'institution dispose de son propre canal.

Deuxièmement. — Déléguer à la Direction la mise en œuvre du système d'information interne et de la procédure de gestion du canal de signalements du Consortium de l'Institut Ramon Llull, conformément aux dispositions de la loi 2/2023 du 20 février, réglementant la protection des personnes qui signalent des infractions réglementaires, la lutte contre la corruption, ainsi que le règlement à approuver pour sa mise en œuvre.

Ce système doit être configuré conformément aux dispositions de l'article 5.2 de la loi 2/2023 et déterminer : le responsable du système, les questions relatives à la procédure, une politique ou une stratégie établissant les principes généraux relatifs au système d'information interne et à la défense du lanceur d'alerte, ainsi que les garanties pour la protection des lanceurs d'alerte dans le cadre de l'institution ».

Par la résolution 007/SII/2023 du 31 juillet 2023, de la Direction générale de la bonne gouvernance, de l'innovation et de la qualité démocratiques, relative au partage, avec le Consortium de l'Institut Ramon Llull, du Système d'alertes interne en matière d'infractions réglementaires et de conduites contraires à l'intégrité publique de l'Administration du Gouvernement de Catalogne, il est décidé :

1. D'autoriser le partage du Système d'alertes interne de l'Administration du Gouvernement de Catalogne avec le Consortium de l'Institut Ramon Llull, et ce à titre transitoire, jusqu'à ce que son propre Système d'alertes interne soit opérationnel, soit, au plus tard, jusqu'au 31 janvier 2024.

2. Ce partage implique que l'entité concernée accepte, sans condition, les principes généraux qui l'inspirent, les garanties d'indemnisation des lanceurs d'alerte, le canal d'alertes interne, la procédure de gestion et la désignation du responsable du Système, qui est également unique, ainsi que toute modification des composantes du Système que l'organisme compétent pourrait effectuer

3. Le partage du Système d'alertes interne n'implique aucune compensation ou contrepartie financière.

4. L'entité doit inclure sur son site Internet un lien vers le Système d'alertes interne de l'Administration du Gouvernement de Catalogne.

5. L'entité doit informer l'Office antifraude de Catalogne du partage du Système d'alertes interne avec l'Administration du Gouvernement de Catalogne, en indiquant que le responsable est le chef de l'unité chargée de la bonne gouvernance qui exerce des fonctions identiques ou similaires à celles de la sous-direction générale.

6. L'organe directeur de l'institution peut décider à tout moment de ne plus partager ce système en le notifiant à cette direction générale et en convenant, d'un commun accord, des mesures transitoires garantissant la continuité du système et l'attention portée aux alertes.

7. Le partage du système prendra effet le lendemain de la signature de la présente résolution.

Compte tenu de ce qui précède, ce texte est présenté, le 21 décembre 2023, à la réunion du Conseil de direction du Consortium de l'Institut Ramon Llull, en vue de l'approbation du Système d'alertes interne du Consortium et du protocole de gestion correspondant, avec une date de référence au 1er février 2024 pour la mise en œuvre de ce Système d'alertes interne, aux fins de mettre en place la Boîte éthique avec l'AOC et de coordonner les mesures transitoires susceptibles de garantir la continuité du système et l'attention portée aux alertes avec la Direction générale de la bonne gouvernance, de l'innovation et de la qualité démocratique.

2. OBJET DU SYSTÈME INTERNE D'INFORMATION

Conformément à la législation en vigueur, et afin de promouvoir une culture d'entreprise basée sur le respect de l'éthique et de la réglementation, ainsi que de prévenir, détecter et réagir aux infractions à la loi, le Consortium de l'Institut Ramon Llull a établi un protocole pour la gestion du Système d'information interne.

L'objectif est d'établir une procédure de gestion du Système d'information interne et de toutes les informations reçues par quiconque, dans le cadre de son travail ou de sa profession, souhaite révéler des faits contraires à la loi et/ou des comportements contraires à l'intégrité publique. Afin de rendre possible cette tâche préventive, la coopération de chacun d'entre nous en matière de détection d'éventuelles conduites irrégulières est fondamentale.

L'existence de ce Système interne n'exclut pas le dépôt de signalements par le biais d'autres canaux externes au niveau européen, national ou régional, tels que l'Autorité indépendante pour la protection du lanceur d'alerte, qui, en Catalogne, est l'Office de lutte antifraude.

Le présent protocole a été élaboré dans le cadre des lignes directrices et des principes énoncés dans la directive (UE) 1937/2019 du 23 octobre 2019 relative à la protection des personnes qui signalent des infractions au droit de l'Union (« Directive Protection des lanceurs d'alerte ») et de sa transposition, par le biais de la loi 2/2023 du 20 février 2023 qui réglemente la protection des personnes qui signalent des infractions aux règles, et vise à lutter contre la corruption (« Loi de protection du lanceur d'alerte »).

3. CHAMP D'APPLICATION

3.1. CHAMP D'APPLICATION PERSONNEL

Toute personne physique ayant obtenu des informations sur des actes répréhensibles dans le cadre de son travail ou de sa profession peut faire un signalement auprès du Système interne. Sont concernées les personnes qui travaillent pour l'entité, que ce soit dans le cadre d'un emploi, d'une relation professionnelle ou d'une relation de service, qu'elle soit temporaire ou permanente, rémunérée ou non. Cette catégorie comprend également les bénévoles, les boursiers/es et les personnes en cours de formation, qu'ils soient rémunérés ou non. Sont également incluses les personnes dont la relation de travail n'a pas encore débuté, lorsque les informations sur les infractions ont été obtenues au cours de la procédure de sélection.

3.2. CHAMP D'APPLICATION MATÉRIEL

Conformément à ce qui précède, l'entité canalisera et facilitera la formulation sécurisée de toute communication concernant:

1. Toutes les actions ou omissions susceptibles de constituer une infraction au droit de l'Union européenne, à condition que:
    - Elles relèvent du champ d'application des actes de l'Union européenne énumérés à l'annexe de la directive (UE) 2019/1937 relative à la protection des personnes qui signalent des violations du droit de l'Union européenne.
    - Affectent les intérêts financiers de l'Union européenne tel que l'établit l'article 325 du Traité sur le fonctionnement de l'Union européenne (TFUE).
    - Ont une incidence sur le marché intérieur, comme en fait état l'article 26.2 du TFUE.
2. Toutes les actions ou omissions susceptibles de constituer une infraction pénale ou administrative grave ou très grave ou une violation du reste de l'ordre juridique.
3. Toutes les actions contraires aux politiques, protocoles, procédures et codes internes que l'entité a établis en matière de conformité réglementaire.
4. Toute opération, tout incident ou tout risque suspect en termes de « prévention du blanchiment de capitaux et du financement du terrorisme » de fraude, de corruption ou d'existence de conflits d'intérêts.

Le Système d'information interne doit être considéré comme un instrument permettant de signaler des irrégularités ou des manquements. Il ne doit donc pas être utilisé sans discernement, mais uniquement aux fins pour lesquelles il a été conçu.

Le Système est présenté comme un outil confidentiel (point 7), dont l'utilisation n'entraînera pas de représailles (point 8).

4. PRINCIPES DU SYSTÈME D'INFORMATION INTERNE

Les principes qui guident le Système d'information interne sont les suivants:

1. Principe de confidentialité (point 7) : les informations relatives aux données, aux lanceurs d'alerte, aux personnes concernées ou aux tiers fournissant des informations, ainsi que les actions de suivi, sont traitées de manière confidentielle.
2. Principe d'anonymat : le droit de soumettre des informations anonymement.
3. Principe de contradiction : il figure parmi les droits des mis/es en cause, auxquels sont accordés l'accès au dossier et la possibilité de soumettre des preuves, ainsi que dans la réglementation des procédures d'audition, d'allégations et de notification à l'issue de la procédure
4. Principe de publicité : le Système d'information interne doit offrir des informations adéquates de manière claire et facilement accessible sur les canaux existants.

Principe d'impartialité : le système interne doit garantir l'impartialité des personnes intervenant dans la gestion des informations.

5. RESPONSABLE DU SYSTÈME D'INFORMATION INTERNE

Le responsable du Système d'information interne doit exercer ses fonctions de manière indépendante et autonome par rapport au reste des organes de l'entité, sans recevoir d'instructions d'aucune sorte dans l'exercice de celles-ci, et il doit disposer de tous les moyens personnels et matériels nécessaires à leur accomplissement

Le/la responsable du Système d'information interne de l'Institut Ramon Llull est la personne qui exerce la Direction de l'entité ; ses fonctions sont les suivantes:

A. Veiller à ce que les infractions soient signalées avec une garantie d'indemnisation et de confidentialité.
B. Fournir des informations sur les éléments constitutifs du système et garantir leur accessibilité dans le domaine du travail ou de la profession.
C. Gérer et suivre les informations reçues conformément à la procédure établie.
D. Préparer le rapport de suivi et le transmettre à l'organe directeur compétent.
E. Établir la communication avec les lanceurs d'alerte.
F. Assurer des mesures de protection et de soutien aux personnes qui fournissent des informations, ainsi qu'à celles qui peuvent se voir affectées pendant le suivi des informations.
G. Établir le rapport annuel sur la reddition des comptes du système.
H. Superviser l'environnement technologique du système.
I. Exercer la fonction de responsable du traitement des données personnelles dérivées du traitement du système.

6. MODE DE PRÉSENTATION DES SIGNALEMENTS

Les signalements peuvent être présentés de manière anonyme ; si ce n'est pas le cas, l'identité du lanceur d'alerte demeure confidentielle. Ils peuvent être déposés de la manière suivante :

- Par écrit : par le biais du canal interne créé à travers la Boîte éthique fournie par l'Administration ouverte de Catalogne, et accessible depuis le site Internet de l'organisation. Ce canal permet de déposer des signalements de manière anonyme.
- Verbalement : par le biais d'une réunion en face à face, à la demande du lanceur d'alerte dans un délai maximum de 7 jours. Les signalements verbaux, avec le consentement préalable du lanceur d'alerte, seront diligentés au moyen de l'enregistrement de la conversation sous un format durable, sécurisé et accessible ou par une transcription complète et précise de la conversation par le personnel chargé de la traiter, le lanceur d'alerte pouvant vérifier, rectifier et accepter la transcription de la conversation en y apposant sa signature.
- L'information peut également être transmise directement, par écrit ou verbalement, au responsable du système et enregistrée dans le Système d'information interne.

Il est recommandé que les signalements présentés contiennent, au minimum, les éléments suivants :

- Identité du/de la mis/es en cause : nom et prénom(s), ainsi que toute autre donnée connue et jugée pertinente pour l'identification de l'auteur/e présumé/e de l'infraction.
- Motif du signalement : description des faits ou des circonstances qui, de l'avis du lanceur d'alerte, constituent un manquement ou une irrégularité.
- Preuves spécifiques à l'appui du signalement : tous les documents disponibles venant étayer la conviction que l'irrégularité décrite dans le motif du signalement a été commise.
- Le cas échéant, le lanceur d'alerte peut indiquer un domicile, une adresse électronique ou un lieu sûr pour recevoir les notifications. De même, le lanceur d'alerte peut à tout moment renoncer expressément à recevoir toute communication concernant les actions entreprises à la suite du signalement.

En tout état de cause, la présentation d'un signalement doit être véridique et étayée par un minimum de justifications, ce qui implique :

- La véracité des faits rapportés, même s'ils ne reposent que sur des doutes ou des soupçons raisonnables et non sur des preuves.
- Que ces faits relèvent bien des champs d'application personnel et matériel.

7. RÉCEPTION DU SIGNALEMENT

7.1. ACCUSÉ DE RÉCEPTION

Après réception d'un signalement, un accusé de réception doit être envoyé à son auteur, via le moyen par lequel il a été déposé, dans un délai maximum de 7 jours ouvrables à compter du lendemain de sa réception, à moins que ce soit impossible parce que le signalement est anonyme, que la personne a renoncé au droit de recevoir des communications ou que cela pourrait compromettre la confidentialité de la communication.

En cas de signalement de l'un des comportements que prévoit le Protocole pour la prévention, la détection, l'action et la résolution des situations de harcèlement sexuel fondées sur le sexe, le genre, l'identité de genre, l'expression de genre et l'orientation sexuelle, le signalement sera activé selon la procédure décrite dans le Protocole.

7.2. RÉCEPTION ET ENREGISTREMENT

L'institution tient un registre des informations reçues et des enquêtes internes réalisées, en garantissant, dans tous les cas, les exigences de confidentialité prévues par la loi.

Conformément à ce qui précède, pour chaque signalement reçu, un dossier sera ouvert et enregistré dans le Système de gestion des signalements, en lui attribuant un code d'identification. Ce Système se trouve dans une base de données sécurisée dont l'accès est restreint.

7.3. ANALYSE DE LA RECEVABILITÉ OU DE L'IRRECEVABILITÉ

Une fois le signalement enregistré, le responsable du Système doit procéder dans un délai inférieur à 10 jours ouvrables à une première évaluation de la recevabilité afin de déterminer si le signalement expose de manière claire et évidente des faits constitutifs d'une infraction. La personne responsable du système peut procéder à toute enquête préliminaire qu'elle juge nécessaire. En fonction des résultats, le responsable doit:

- Rejeter le signalement par le biais d'une résolution motivée dès lors que:
    - Les fait communiqués semblent invraisemblables ou dénués de fondement.
    - Les faits décrits ne relèvent pas du champ d'application matériel ou personnel.
    - Les faits ne permettent pas d'identifier l'infraction. La personne responsable du système peut demander des informations complémentaires ou des précisions sur les faits. En l'absence de réponse dans un délai de 10 jours ouvrables, la demande est rejetée.
    - Lorsque les faits ont déjà fait l'objet d'actions antérieures ou lorsqu'il existe une décision de justice en la matière.
    - Lorsqu'il existe des motifs raisonnables de suspecter que l'information a été obtenue par la commission d'un délit ou que les faits rapportés constituent un délit, au lieu de se borner simplement à refuser de traiter le signalement, le responsable du canal interne des signalements doit gérer immédiatement l'information et la transmettre à la fois à la Direction de l'entité et au ministère public.
- Admettre le signalement pour traitement.

L'acceptation ou le rejet du signalement est notifié au lanceur d'alerte dans les cinq jours ouvrables suivants, à moins que le signalement soit anonyme, que la personne ait renoncé au droit de recevoir des communications ou que la confidentialité de la communication risque d'être compromise. Lors de la communication du refus, la possibilité d'utiliser le canal de signalement externe de l'Office antifraude de Catalogne ou de divulguer publiquement les faits doit être mentionnée.

Le responsable du Système informe la Direction de l'entité de la réception du signalement, à condition qu'elle ne soit pas elle-même impliquée dans les faits dénoncés. Si elle l'est, il en informe la personne qui est la plus représentative des organes de direction et n'a aucun rapport avec les faits.

Enfin, le responsable du système est tenu de garder absolument confidentiel tout signalement reçu, qu'il soit rejeté ou non, notamment en ce qui concerne le lanceur d'alerte et le/la mis/e en cause, en s'abstenant de promouvoir tout type de représailles à l'encontre du lanceur d'alerte.

7.4. ENQUÊTE

Une fois le signalement reçu et accepté, le responsable du système ordonne l'ouverture de l'enquête interne correspondante, dans le but de:

- Clarifier les faits signalés.
- Identifier les responsables des comportements signalés.
- Rassembler les preuves nécessaires à leur révélation.

L'enquête doit être menée dans les plus brefs délais. L'enquête ne doit pas se prolonger au-delà de 3 mois à compter de la réception du signalement, ou, si aucun accusé de réception n'a été adressé au lanceur d'alerte, 3 mois à compter de l'expiration du délai de 7 jours après la communication. Une prolongation extraordinaire pouvant aller jusqu'à 3 mois supplémentaires peut être autorisée, lorsqu'elle est proportionnée à la nature et à la complexité des faits enquêtés, en dictant une résolution motivée à cet effet.

Au cours de la procédure d'enquête, le responsable du système effectue toutes les actions et consultations qu'il juge nécessaires pour déterminer l'exactitude et la véracité des informations reçues, ainsi que pour clarifier les faits.

Le responsable du système prend contact avec le/la mis/e en cause, en se présentant comme la personne chargée d'enquêter sur le signalement et en l'informant succinctement des faits qui lui sont reprochés et des principales étapes de l'enquête. De même, dans cette communication, on l'informe de la possibilité de présenter des allégations par écrit et d'être informé/e du traitement de ses données personnelles. Cette communication doit intervenir dans les délais et de la manière jugés appropriés pour assurer la bonne fin de l'enquête.

En aucun cas les mis/es en cause ne sont informés de l'identité de la personne qui a déposé le signalement, lequel ne sera pas dévoilé afin de protéger le lanceur d'alerte.

Au cours de l'enquête, toutes les actions licites et valables du point de vue juridique peuvent être menées afin de faire la lumière sur les faits objet du signalement, dans le respect du principe de proportionnalité, à condition que la mesure soit exceptionnelle (absence d'autres mesures d'enquête moins onéreuses pour atteindre l'objectif poursuivi), nécessaire (sans elle, l'enquête pourrait être compromise) et appropriée (elle doit servir les objectifs de l'enquête).

Tous/tes les employé/es et les membres des organes directeurs de l'entité sont tenus/es de prêter la coopération requise, de collaborer à l'enquête, leur intervention étant tenue strictement confidentielle.

Les moyens d'investigation licites sont les suivants:

1. Entretien avec la ou les mis/es en cause, précédé d'une lecture des droits et des garanties dont ils disposent :
    - Droit d'être informé/e des faits faisant l'objet de l'enquête et d'être entendu/e à tout moment.
    - Droit d'accès au dossier d'enquête, sans révéler d'informations permettant d'identifier le lanceur d'alerte.
    - Droit de savoir si l'entretien sera enregistré et consigné.
    - Droit de formuler des allégations par écrit et de proposer des mesures d'enquête
    - Droit à la présomption d'innocence et à l'honneur.
2. Entretien avec le lanceur d'alerte, si possible, précédé de l'avertissement relatif à l'interdiction de tout type de représailles ou de tentative de représailles à la suite du signalement déposé. Mention devra être faite de l'éventuelle nécessité de maintenir la communication tout au long de l'enquête et de demander des informations supplémentaires à l'intéressé/e.
3. Interroger les témoins qui peuvent avoir connaissance ou être témoins des faits rapportés
4. Examen de tout type de documents et demande de documents aux personnes physiques ou morales correspondantes.
5. Recueil et analyse des informations contenues dans les dispositifs électroniques, grâce à l'utilisation de logiciels et de machines préservant l'intégrité des preuves, dans le respect de la législation en vigueur.
6. Si cela est indispensable à l'élucidation des faits, adopter des mesures de surveillance par le biais de détectives ou de moyens informatiques, télématiques ou audiovisuels, à condition qu'ils soient conformes aux critères de raisonnabilité, d'adéquation et de proportionnalité, en garantissant à tout moment le droit à la vie privée de l'employé et le droit au secret des communications.
7. Demander une assistance externe à d'autres professionnels.
8. Toute autre mesure que l'enquêteur/trice jugerait nécessaire pour clarifier les faits.

À l'issue de tous les entretiens réalisés, un procès-verbal de la réunion est rédigé et signé par la personne interrogée pour attester de son accord. Des preuves de toutes les actions menées sont également collectées

À l'issue de l'enquête, les personnes concernées par le signalement sont entendues. Un délai de quinze jours ouvrables est établi pour que la personne concernée par le signalement présente les allégations qu'elle juge appropriées et propose, le cas échéant, les moyens de preuve qu'elle juge pertinents.

8. CLÔTURE DE LA PROCÉDURE

Une fois que toutes les actions ont été menées à bien, le responsable du Système émet un rapport motivé qui contient au moins les éléments suivants :

- Un exposé des faits signalés.
- Les actions menées dans le but de clarifier les faits, l'évaluation des preuves recueillies et les indices obtenus.
- Les conclusions des enquêtes, avec l'identification de la déficience qui, le cas échéant, a occasionné la situation et la proposition d'un plan d'action pour y remédier.
- Proposition de remettre toutes les actions à l'organe compétent ou classement des actions si l'enquête n'a pas permis de réunir des informations nécessitant une action supplémentaire en raison de l'absence de preuves suffisantes de la commission présumée d'un délit ou, en tout état de cause, si les faits, en raison de leur insignifiance, ne doivent pas donner lieu à une action supplémentaire. Dans ce cas, il est décidé de classer l'affaire, assortie d'une explication motivée et détaillée, en notifiant cette décision au lanceur d'alerte et, le cas échéant, à la personne mise en cause.

La venue à échéance du délai limite pour notifier le rapport n'a aucun effet du point de vue juridique. Seule l'auteur/e du signalement peut choisir différentes façons de le communiquer, notamment le recours au canal externe de l'Office antifraude de la Catalogne ou la révélation publique.

9. PROTECTION DU LANCEUR D'ALERTE EN CAS DE REPRÉSAILLES

Les personnes qui communiquent, de bonne foi et dans les conditions prévues dans le présent document, des informations sur le non-respect des règles sont protégées contre toute forme de représailles, de discrimination et de pénalisation en raison des informations communiquées. Aussi les actes constituant des représailles, y compris les menaces et les tentatives de représailles, sont-ils expressément interdits.

Pour davantage de clarté, on entend par représailles tous les actes ou omissions proscrits par la loi ou qui, directement ou indirectement, impliquent un traitement défavorable mettant les personnes qui en sont victimes dans une situation de désavantage particulier par rapport à d'autres dans le contexte du travail ou de la profession, simplement en raison de leur statut de lanceur d'alerte, ou parce qu'elles ont révélé des faits publiquement.

10. CONFIDENTIALITÉ ET PROTECTIONS DES DONNÉES À CARACTÈRE PERSONNEL

Cette entité documente par écrit toutes les actions entreprises dans le cadre des signalements de manquements et du traitement du dossier correspondant, et en assure la conservation conformément aux exigences de confidentialité, aux mesures de sécurité et aux conditions de conservation établies par d'autres réglementations obligatoires.

Le traitement des données à caractère personnel effectué en vertu des actions menées dans le cadre du présent protocole est régi par les dispositions du règlement UE 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (règlement général sur la protection des données ou RGPD), de la loi organique 3/2018, de 5 décembre sur la protection des données et des droits numériques (LOPDGDD), et de la loi organique 7/2021 du 26 mai sur la protection des données personnelles traitées aux fins de prévenir, détecter, enquêter et juger les infractions pénales et exécuter les sanctions pénales, et autres règles applicables. À cet égard, aucune donnée personnelle ne sera collectée si elle n'est pas pertinente et nécessaire à l'enquête et à la résolution de l'affaire signalée.

Afin d'atteindre un niveau maximal d'implication et de sécurité pour la personne qui souhaite signaler une infraction ou un comportement irrégulier par l'intermédiaire du Système d'information interne, ainsi que pour la personne mise en cause, l'institution doit fournir les moyens nécessaires pour garantir que les communications au système d'information interne sont traitées avec la plus grande confidentialité par toutes les personnes impliquées dans l'enquête et la résolution de l'affaire.

Les personnes qui effectuent une communication par l'intermédiaire du Système d'information interne déclarent et garantissent que les données personnelles fournies sont véridiques, exactes, complètes et à jour, et dégagent l'entité de toute responsabilité pouvant découler du non-respect de ces déclarations et garanties.

En tout état de cause, les données faisant l'objet d'un traitement ne peuvent être conservées dans le système d'information interne que le temps nécessaire pour décider de l'opportunité d'ouvrir une enquête sur les faits signalés.

- S'il est prouvé que tout ou partie de l'information fournie n'est pas véridique, elle est immédiatement supprimée dès l'instant où l'on en a connaissance, même si ce manque de véracité peut constituer un délit pénal, et dans ce cas, l'information est conservée le temps nécessaire à l'exécution de la procédure judiciaire.
- En tout état de cause, si trois mois se sont écoulés depuis la réception de la communication sans qu'aucune mesure d'enquête n'ait été prise, les informations doivent être supprimées, à moins que le but de la conservation soit de laisser des preuves du fonctionnement du système.
- Nonobstant ce qui précède, le responsable du système est chargé de classer et de conserver toute la documentation qui en découle dans le registre pendant une période de cinq ans à compter de la réception de la notification ou du signalement.
- En tout état de cause, les données sont conservées sous forme bloquée, c'est-à-dire qu'elles sont identifiées et réservées afin d'en empêcher le traitement, à moins qu'il faille les mettre à la disposition des administrations publiques, des juges et des tribunaux. Les communications qui n'ont pas été admises ne peuvent être enregistrées que de manière anonyme, et l'obligation de blocage prévue à l'article 32 de la loi organique 3/2018 du 5 décembre, ne leur est pas applicable.

Le Consortium de l'Institut Ramon Llull traite les données obtenues par le biais du Système d'information interne en tant que responsable du traitement aux fins suivantes:

- Enregistrement des communications sur les actions ou omissions, dans la sphère interne de l'activité du Consortium, qui peuvent constituer un non-respect de la réglementation,
- Vérification des informations, suivi et élaboration de rapports avec des propositions d'action,
- Communication avec les lanceurs d'alerte et les mis/es en cause.
- Communication, si nécessaire, à l'autorité judiciaire, au ministère public ou à l'autorité administrative compétente.

Les données sont traitées sur la base du respect de l'obligation légale (art. 6.1.c RGPD) et peuvent être communiquées aux destinataires détaillés ci-dessus.

Pour exercer leurs droits d'accès, de rectification, d'effacement, d'opposition, de limitation du traitement, dans les cas prévus par la loi, dans les termes prévus par la législation en vigueur, les intéressés peuvent s'adresser à l'entité en envoyant une communication écrite à dpd@llull.cat. De même, des informations complémentaires et détaillées sur l'exercice des droits et le traitement des données personnelles peuvent être consultées dans la politique de protection des données publiée sur www.llull.cat.

11. VALIDITÉ

Le Système d'alertes interne du Consortium de l'Institut Ramon Llull entre en vigueur le 1er février 2024, sachant que la validité de l'autorisation de partager, à titre transitoire, le Système d'alertes interne de l'Administration du Gouvernement de Catalogne avec le Consortium de l'Institut Ramon Llull est fixée, au maximum, au 31 janvier 2024.

En ce sens, si nécessaire, les mesures transitoires correspondantes peuvent être adoptées pour garantir la continuité du système et l'attention portée aux alertes avec la Direction générale de la bonne gouvernance, de l'innovation et de la qualité démocratique, ainsi que la mise en service effective du service de Boîte éthique avec l'AOC.

À partir de son entrée en vigueur, le présent protocole reste valide pour une durée indéterminée, sans préjudice des éventuelles modifications et améliorations qui pourraient y être introduites.

www.llull.cat | @IRLlull