# Gestion des alertes

# Mode d'emploi

Table des matières



État au 17 novembre 2017

# 1. Introduction

## 1.1. Définition du concept

Le Conseil de l'Europe définit le lanceur d'alerte (« whistleblower ») comme « toute personne qui fait des signalements ou révèle des informations concernant des menaces ou un préjudice pour l'intérêt général dans le contexte de sa relation du travail, qu'elle soit dans le secteur public ou le secteur privé ». Il s'agit d'une personne qui transmet aux autorités d'importantes informations issues d'un contexte confidentiel ou protégé et qui permettent la découverte de dysfonctionnements.

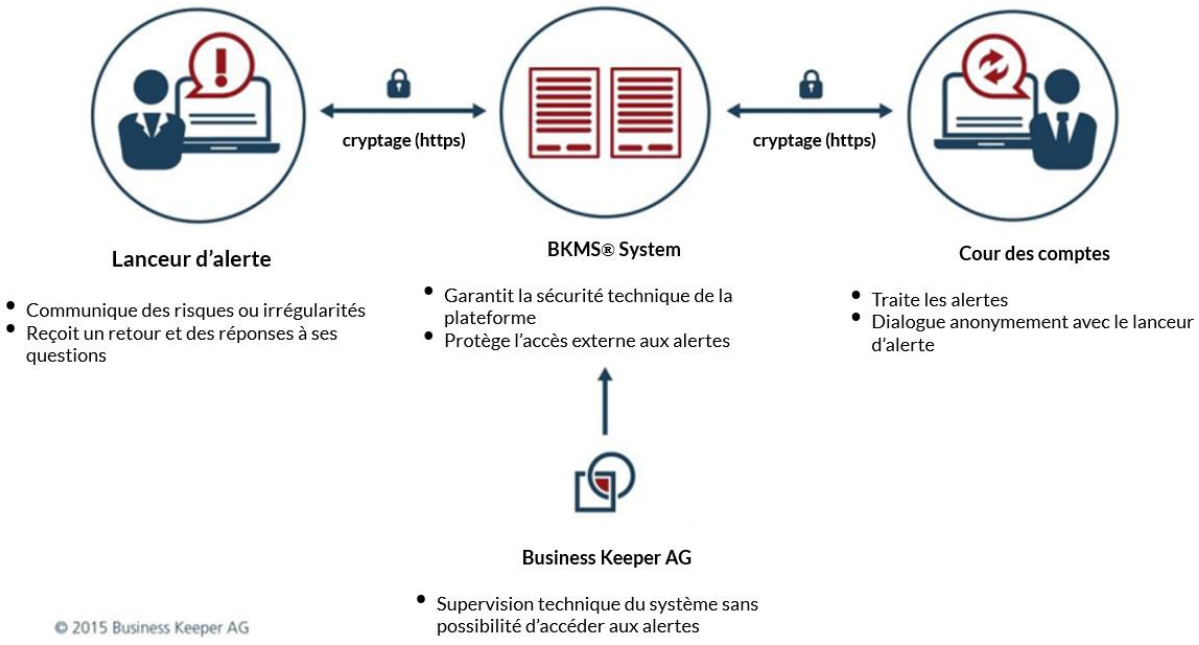
## 1.2. Historique

Depuis sa création, la Cour des comptes a reçu plusieurs centaines de communications de tiers. D'abord par courrier, puis également par courriel et via un formulaire de contact web hébergé hors État de Genève. Actuellement, ces alertes sont reçues au rythme de plus d'une par semaine et sont à l'origine de plus de la moitié des rapports de la Cour.

Parmi ces communications, la Cour a été informée de soupçons de corruption ou d'usage privé de biens publics, d'abus dans les systèmes de rémunération ou de notes de frais, de favoritisme dans les attributions de mandats, de dysfonctionnements dans la gestion de projets, d'indices d'irrégularité dans les marchés publics ou d'attributions arbitraires de logements par une institution publique. Les conséquences ont pu se traduire par des dépenses inappropriées pour l'État, des inégalités de traitement dans l'octroi de prestations ou encore par la violation de lois dans certains domaines. C'est dire que pour des informations d'une telle sensibilité, la Cour des comptes se doit d'offrir des possibilités de communication garantissant une totale confidentialité, comme le prévoit d'ailleurs sa base légale (art. 28 al. 2 LSurv : « La confidentialité de l'identité de la personne lui est garantie. »)

## 2. Fonctionnement du système BKMS®

Le système BKMS® permet une communication bidirectionnelle avec un lanceur d'alerte anonyme au moyen d'une boîte aux lettres protégée prévue à cet effet. Le lanceur d'alerte signale les risques et les abus et peut converser avec la Cour des comptes (receveur d'alerte) de manière anonyme via le système BKMS®. Ce système permet ainsi de relier deux termes opposés en apparence : anonymat et dialogue.




Source : Business Keeper AG, traduction par la Cour des comptes

Le système BKMS® enregistre des signalements à l'échelle mondiale 24h/24. Chaque signalement est sauvegardé sur le serveur BKMS® au moyen d'un cryptage individuel et ne peut être déchiffré que par la Cour des comptes, en tant que client de Business Keeper AG. Le système BKMS® n'est pas une adresse courriel mais permet une communication indirecte entre le lanceur d'alerte et la Cour des comptes via le serveur BKMS®. Business Keeper AG n'a pas accès aux messages et données du lanceur d'alerte.

Le système BKMS® et ses fonctions sont présentés dans cette vidéo.

## 3. Anonymat : une priorité

### 3.1. Dilemme du lanceur d'alerte

La découverte d'un état de fait par un lanceur d'alerte est appréciée de façon différente par le grand public. D'un côté, le lanceur d'alerte peut être vu comme un dénonciateur, d'un autre côté, il est considéré comme une personne courageuse qui contribue à la lutte contre la criminalité. Ce dilemme dépend surtout de la façon dont les informations pertinentes sont présentées.

Deux possibilités s'offrent à un lanceur d'alerte potentiel : soit il choisit de dénoncer le comportement répréhensible, soit il choisit de le taire. Le devoir de fonction impose de solliciter la hiérarchie en premier lieu. Toutefois, il arrive que la hiérarchie ne prenne pas de mesures suffisantes ou soit directement incriminée dans la situation répréhensible. Afin de prendre la bonne décision, le lanceur d'alerte va alors peser les avantages et les inconvénients de sa déclaration : manifestation de son propre sentiment de justice, préservation de gaspillages pour la collectivité, mais aussi crainte de devoir endurer des représailles telles que l'intimidation, l'isolement, la diffamation ou la discrimination si son identité venait à être révélée. La possibilité pour le lanceur d'alerte de préserver son anonymat en communiquant via une boîte aux lettres spécifique dans le cadre de l'utilisation du système BKMS® réduit sa crainte de communiquer des renseignements et sert à la protection contre d'éventuelles représailles.

### 3.2. Garantie de l'anonymat du lanceur d'alerte

Le système BKMS® a été développé sur la base d'un concept ASP (Application Service Providing). Cette application, fournie par le prestataire de services de Business Keeper AG, propose l'utilisation du système BKMS® sur le Web et est responsable de toute l'administration informatique du système, en particulier de la garantie de la protection des données.

#### *3.2.1.* Sécurité *technique*

Chaque communication sur le Web s'effectue sur la base d'un protocole internet (IP). Dans un réseau informatique, chaque appareil doit avoir une adresse unique : l'adresse IP.

Le système BKMS® a également besoin d'adresses IP. Celles-ci ne sont cependant utilisées qu'au moment de la matérialisation de la réponse aux demandeurs et ne sont ensuite plus disponibles. Les indications de temps, les données de géolocalisation et les autres métadonnées du lanceur d'alerte ne sont pas enregistrées. Il n'est pas non plus possible de savoir à qui la réponse a été envoyée ou de quelle adresse proviennent les données transmises. Ces processus sont solidement ancrés dans le logiciel ; ils ne peuvent pas être modifiés et garantissent la sécurité du système.

Les données du lanceur d'alerte créées lors de l'établissement de la boîte aux lettres sont cryptées, ce qui signifie que les identifiants ne peuvent pas être lus. Chaque information est codée séparément.

En résumé, l'anonymat du lanceur d'alerte est protégé et le décryptage d'informations par un tiers ou par Business Keeper AG n'est pas possible.

#### *3.2.2. Sécurité physique*

Le système BKMS® est exploité dans des *data center* de haute sécurité au sein de l'UE et en Suisse. La sécurité de l'exploitation du serveur informatique est assurée grâce à une reconnaissance automatique des dysfonctionnements de l'équipement informatique. L'administration et la maintenance du serveur incombent exclusivement à Business Keeper AG. Les serveurs contiennent uniquement ce qui est nécessaire à l'utilisation et au maintien du système BKMS®. Ils sont dotés d'importants mécanismes de séparations et de cryptage, de sorte qu'un mélange de données est exclu.

### 3.3. Devoir de diligence du lanceur d'alerte

L'anonymat d'un lanceur d'alerte est, comme cela vient d'être présenté, assuré du point de vue technique. Cela étant, aucun moyen technique ne peut assurer l'anonymat d'un lanceur d'alerte si celui-ci ne s'acquitte pas de son devoir de diligence.

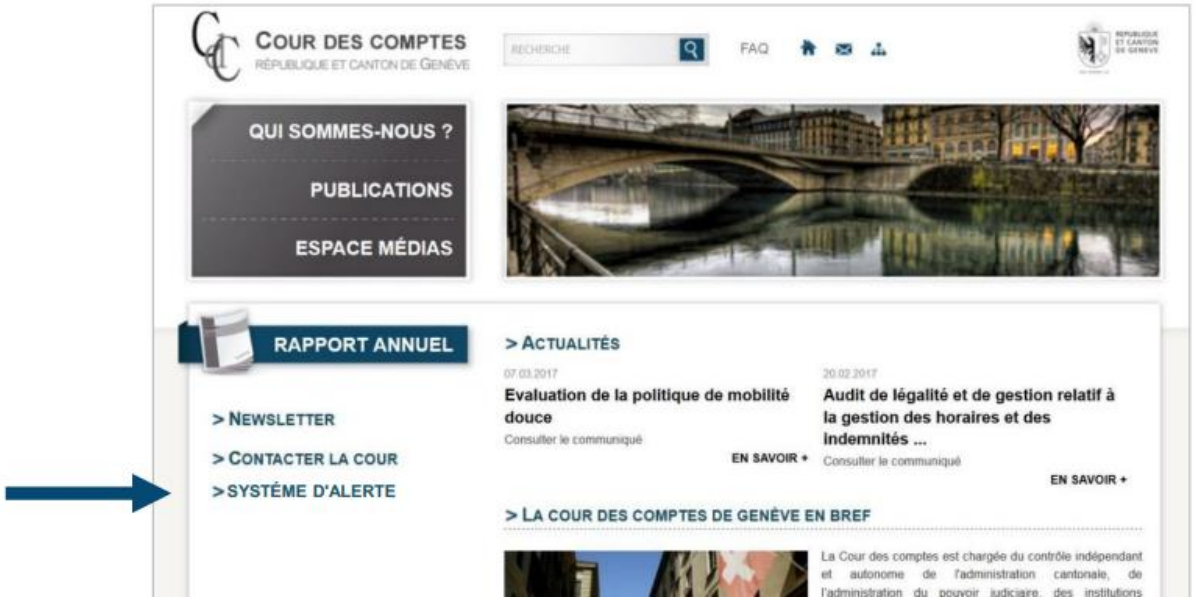
Ce devoir de diligence est rappelé plusieurs fois au lanceur d'alerte lors du processus de signalement. Ainsi, lors des différentes étapes de la procédure, il est demandé au lanceur d'alerte de ne pas transmettre de signalements sur un réseau interne ou des données qui permettraient son identification. Une description trop détaillée d'un état de fait, une transmission d'annexes en version numérique avec des métadonnées, ou encore la mention de son propre nom, mettent en péril l'anonymat du lanceur d'alerte.

Les lanceurs d'alerte qui ne souhaitent pas préserver leur anonymat bénéficient du devoir de confidentialité de la Cour. L'article 28 de la loi sur la surveillance de l'État garantit aux personnes qui s'adressent à la Cour la confidentialité quant à leur identité et les renseignements recueillis sont strictement secrets, en vertu du serment prononcé par les magistrats après leur élection (art. 21 al. 1er LSurv) et par les membres du personnel lors de leur engagement (art. 9A LPAC). Seules les autorités pénales peuvent – sur décision expresse – accéder à des informations détenues par la Cour.

## 4. Signalement d'une alerte dans le système BKMS®

### 4.1. Accessibilité

Le système de collecte d'alerte BKMS® est accessible sur la page d'accueil de la Cour des comptes ou en copiant l'URL https://www.bkms-system.net/cdc.



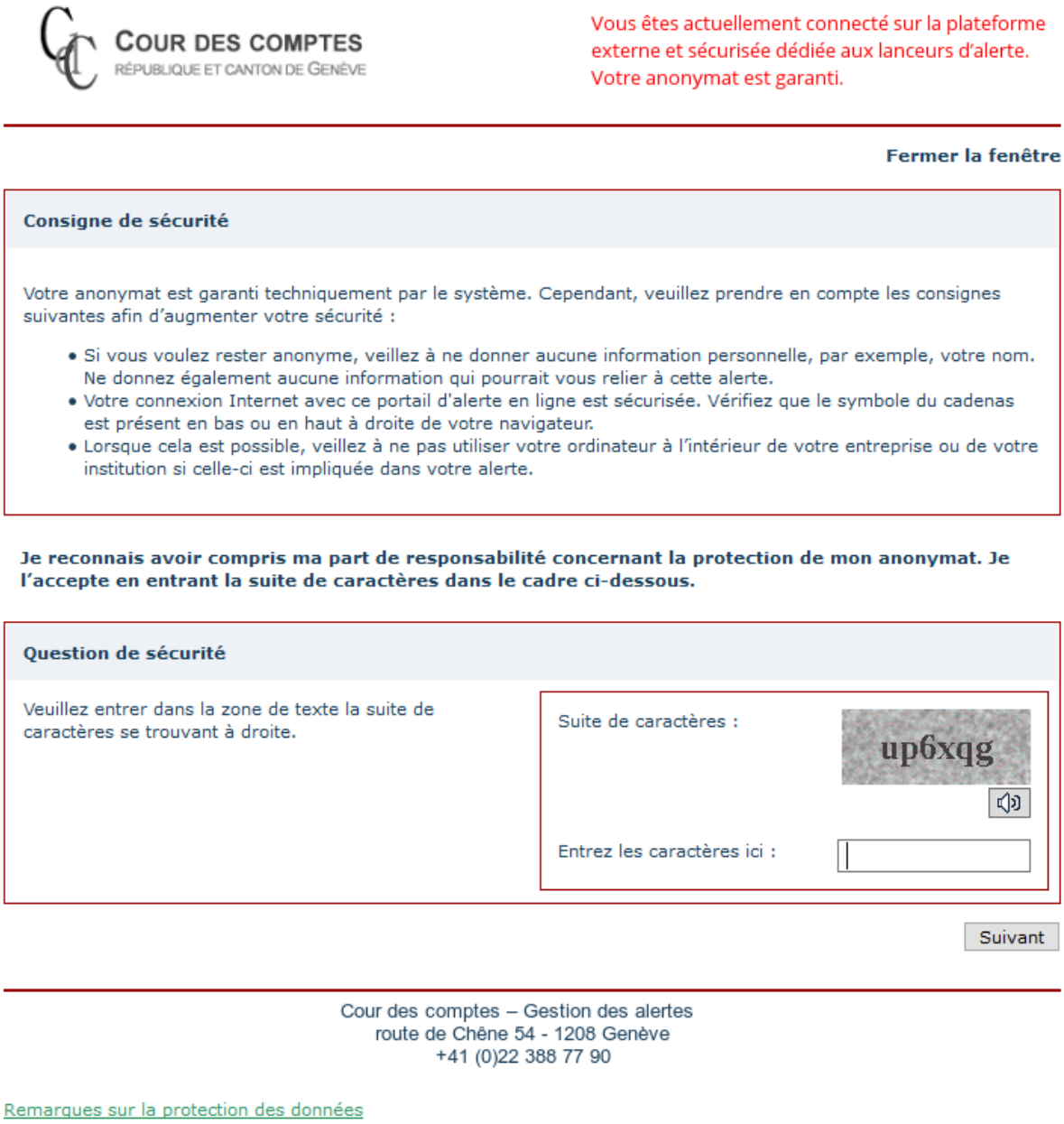
### 4.2. Page d'accueil

La page d'accueil donne des explications et instructions détaillées, mentionnant notamment la possibilité, d'une part, de protéger son anonymat lors de l'utilisation de la plateforme de communication et, d'autre part, de contribuer activement à l'élucidation de soupçons liés à la légalité des activités de l'État ou au bon emploi des fonds publics, voire à des crimes ou à des délits.

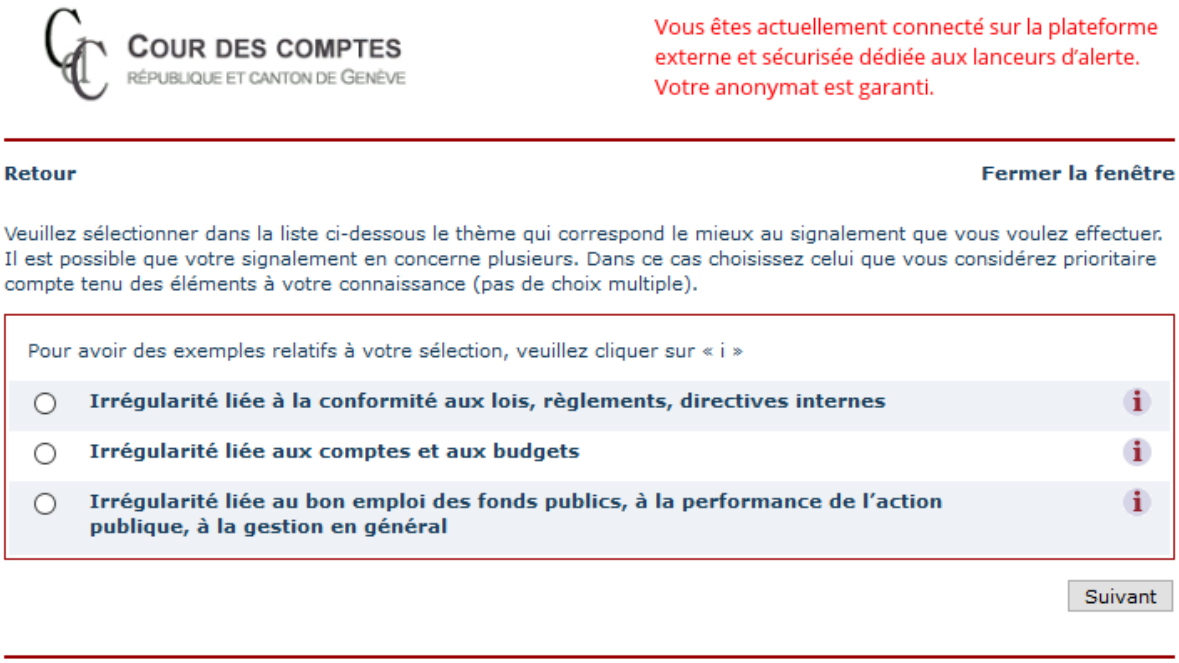
### 4.3. Processus de signalement d'une alerte

En cliquant sur « soumettre une alerte », le processus de signalement se déclenche en quatre étapes.

En premier lieu, on demande au lanceur d'alerte de lire un texte sur la protection de son anonymat ainsi que de recopier manuellement une suite de caractères alphanumériques dans le champ prévu à cet effet, ce qui sert à la protection contre les attaques automatisées.

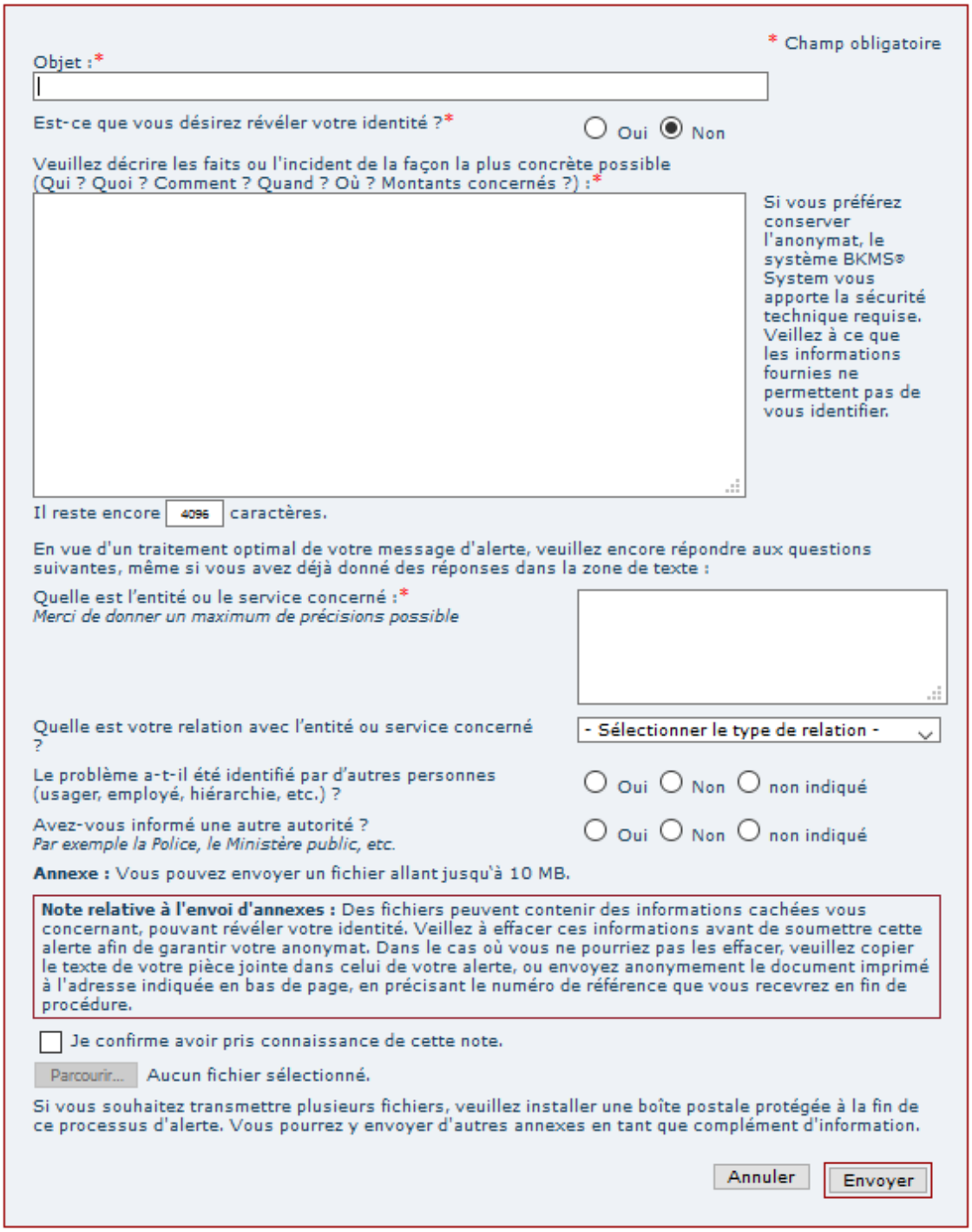


À la page suivante, on demande au lanceur d'alerte le thème principal de son alerte.

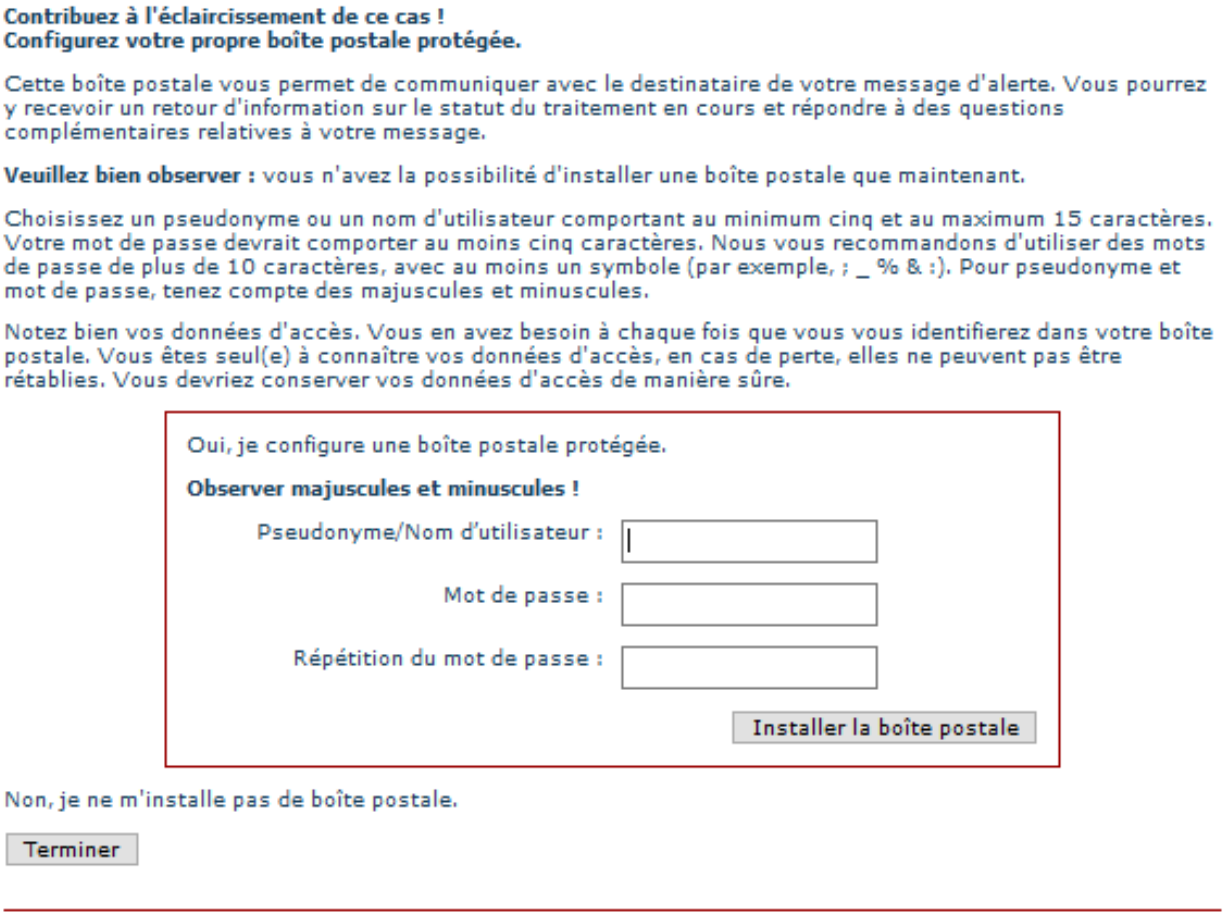


En troisième lieu, le lanceur d'alerte formule son signalement avec ses propres mots. Il a à sa disposition 4'096 signes pour verbaliser son alerte. Il doit également répondre à quelques questions pour que son signalement puisse être efficacement utilisé. Afin de concrétiser l'état de fait, le lanceur d'alerte sélectionne ses réponses parmi une liste déroulante ou par des coches.

Chaque lanceur d'alerte est libre d'envoyer son signalement de manière anonyme ou en donnant son identité. Il doit obligatoirement se prononcer sur cette question. Le lanceur d'alerte peut annexer à son alerte un fichier d'une grosseur de 10 MB au maximum. D'autres annexes peuvent par la suite être rajoutées sur la boîte aux lettres sécurisée. Le lanceur d'alerte peut également apporter des preuves factuelles ou personnelles.



En quatrième lieu, le lanceur d'alerte peut installer sa propre boîte aux lettres protégée en choisissant un nom d'utilisateur et un mot de passe, sur laquelle il peut répondre aux questions posées par la Cour des comptes et obtenir une réaction de sa part, notamment sur l'avancée du traitement de son alerte.



**Contribuez à l'éclaircissement de ce cas !**
**Configurez votre propre boîte postale protégée.**

Cette boîte postale vous permet de communiquer avec le destinataire de votre message d'alerte. Vous pourrez y recevoir un retour d'information sur le statut du traitement en cours et répondre à des questions complémentaires relatives à votre message.

**Veuillez bien observer :** vous n'avez la possibilité d'installer une boîte postale que maintenant.

Choisissez un pseudonyme ou un nom d'utilisateur comportant au minimum cinq et au maximum 15 caractères. Votre mot de passe devrait comporter au moins cinq caractères. Nous vous recommandons d'utiliser des mots de passe de plus de 10 caractères, avec au moins un symbole (par exemple, ; _ % & :). Pour pseudonyme et mot de passe, tenez compte des majuscules et minuscules.

Notez bien vos données d'accès. Vous en avez besoin à chaque fois que vous vous identifierez dans votre boîte postale. Vous êtes seul(e) à connaître vos données d'accès, en cas de perte, elles ne peuvent pas être rétablies. Vous devriez conserver vos données d'accès de manière sûre.

Oui, je configure une boîte postale protégée.

**Observer majuscules et minuscules !**

Pseudonyme/Nom d'utilisateur :

Mot de passe :

Répétition du mot de passe :

Installer la boîte postale

Non, je ne m'installe pas de boîte postale.

Terminer

## 5. Traitement de l'alerte par la Cour des comptes

La force du système BKMS® réside dans le fait que, comparé aux signalements communiqués de façon totalement anonyme, il est ici possible d'entrer en contact avec le lanceur d'alerte sur la boîte aux lettres protégée et de concrétiser l'état de fait. Les réponses du lanceur d'alerte permettent de déterminer à quel point ses affirmations sont étayées et de qualifier ses allégations comme de simples suppositions ou comme ses propres perceptions de l'état de fait. En outre, les premiers actes d'enquête peuvent débuter dès que le signalement est formulé. La communication avec le lanceur d'alerte permet déjà d'apprécier s'il existe vraiment un état de fait contraire au droit, qui rendrait nécessaire le déclenchement d'une procédure d'enquête. D'un côté, ces informations facilitent la découverte de constats plus précis et étayés, de même que la formulation de recommandations ciblées ou la prise de mesures rapides et adéquates. De l'autre côté, des enquêtes pour clarifier de vagues signalements sont évitées, ce qui permet une économie des ressources.

### 5.1. Attribution de l'annonce au sein de la Cour des comptes

Chaque signalement d'un lanceur d'alerte est attribué à un magistrat et à un collaborateur de la Cour des comptes qui traitent la communication. Le système BKMS® est paramétré de façon à contraindre le traitement des alertes par au moins deux personnes de sorte à respecter le principe des quatre yeux. Lorsqu'une boîte aux lettres protégée est installée par le lanceur d'alerte, un accusé de réception est envoyé par la Cour à bref délai.

### 5.2. Examen de l'alerte

La Cour des comptes détermine si les informations communiquées sont suffisantes pour être examinées par le collège des magistrats. Les lanceurs d'alerte dont le signalement présente un niveau de précision ou d'information ne permettant pas à la Cour de réaliser un examen adéquat, font l'objet d'un message par le biais de la boîte aux lettres protégée prévue à cet effet, afin d'essayer d'obtenir plus d'informations.

Dans le cas où les informations reçues, voire les résultats de l'enquête de la Cour, font apparaître des soupçons de crimes ou de délits, la Cour des comptes en avisera le Ministère public, en application de l'art. 33 LaCP et de l'art. 29 al. 1 LSurv. De même, si le lanceur d'alerte est un fonctionnaire ou membre d'une autorité (employé d'une administration cantonale ou communale, employé d'un établissement public, élu, etc.) et qu'il pense être face à un crime ou à un délit poursuivi d'office, il lui est rappelé qu'il a l'obligation d'en aviser sans tarder la police (en se rendant dans un poste de police) ou le Ministère public (par écrit : Ministère public, case postale 3565, 1211 Genève 3), en application de l'art. 33 de la loi d'application du code pénal suisse (LaCP).

Si les communications reçues entrent dans le champ de compétence de la Cour, elles donneront lieu in fine à une analyse. Celle-ci prendra la forme soit d'un examen sommaire, soit d'un audit. Les examens sommaires qui présentent un intérêt public sont publiés intégralement, une synthèse étant rédigée pour les autres dans le rapport annuel. Les audits sont publiés systématiquement. L'ensemble des publications se trouve sur le site internet de la Cour des comptes www.cdc-ge.ch, dans une rédaction qui évidemment préserve l'anonymat des lanceurs d'alerte.