

Cette « frequently asked questions (FAQ) » a pour but de vous aider à mieux comprendre et appréhender le dispositif d'alerte OVH.

1. Pourquoi mettre en place cette plateforme ROGER ?

Dans le cadre de l'article 17 de la loi française Sapin II, la mise en place d'un dispositif d'alerte est destinée à permettre le recueil des signalements émanant de nos parties prenantes et relatifs à l'existence de conduites ou de situations contraires au code éthique d'OVHcloud. Cette disposition de la loi s'applique à toute société française employant plus de 50 salariés.

2. ROGER, de quoi s'agit-il ?

ROGER est l'acronyme de Respect OVHCloud Guidelines & Ethical Rules* (*Respect des bonnes pratiques et des règles éthiques d'OVHcloud). Il s'agit de la plateforme d'alerte d'OVHcloud permettant de signaler tout fait constaté ne respectant pas notre code éthique, ou ne respectant pas nos valeurs. Il peut s'agir par ex de dénoncer des faits liés à la fraude ; à des détournements ou vols ; des dommages environnementaux ; à la santé au travail, l'hygiène et la sécurité ; à des situations de discrimination ou d'harcèlement ; Le non-respect des lois, des règlements ou de l'intérêt général ou concernant les sujets de conflits d'intérêts, corruption et trafic d'influence.

3. Comment accéder à ROGER ?

La plateforme ROGER est accessible à tout moment et depuis n'importe quel appareil : ordinateur, tablette ou smartphone. Pour effectuer une déclaration, il vous suffit de vous connecter sur www.roger.ovh ou go/roger et de suivre les indications.

Dernière précision, www.roger.ovh pointe sur l'url de notre solution externe <https://ovh-group.signalement.net/entreprises> adoptant ainsi le protocole https afin de vous permettre de consulter la plateforme ROGER en toute sécurité, quel que soit son contenu.

4. ROGER est destiné à qui ?

ROGER est ouvert à toute personne qui, dans le contexte de sa relation de travail au sein d'OVHcloud ou dans le cadre de sa relation avec le groupe OVHcloud, souhaite révéler ou signaler un état de fait mettant en lumière des comportements ne respectant pas les valeurs et règles de notre code éthique. Cette personne devient un lanceur d'alerte*.

5. *Qu'est-ce un lanceur d'alerte pour OVHcloud ?

Conformément à la loi, un lanceur d'alerte est une personne physique qui révèle ou signale, de manière désintéressée et de bonne foi, un crime ou un délit, une violation grave et manifeste d'un engagement international régulièrement ratifié ou approuvé par la France, d'un acte unilatéral d'une organisation internationale pris sur le fondement d'un tel engagement, de la loi ou du règlement, ou une menace ou un préjudice grave pour l'intérêt général, dont elle a

eu personnellement connaissance. Les faits, informations ou documents, quel 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 le présent chapitre.

Nous avons souhaité ouvrir cette définition à toute personne souhaitant signaler un comportement inapproprié ou un fait contraire aux valeurs de l'entreprise.

Le lanceur d'alerte est pénalement irresponsable dès lors que les critères de définition fixés par la loi française n° 2016-1691 du 9 décembre 2016 sont remplis, que la divulgation de l'information « est nécessaire et proportionnée à la sauvegarde des intérêts en cause » et qu'elle intervient dans le respect des procédures de signalement des alertes (article 122-9 du code pénal français).

Qu'il soit salarié ou agent public, civil ou militaire, le lanceur d'alerte ne peut être licencié, sanctionné ou discriminé d'aucune manière pour avoir signalé des faits dans le respect de la procédure de signalement des alertes (article L 1132-3-3 du code du travail ; article 6 ter A alinéa 2 de la loi n° 83-634 du 13 juillet 1983 ; article L. 4122-4 alinéa 2 du code de la défense).

6. Quels sont les critères de sécurité et de confidentialité du dispositif ?

Toutes les personnes ayant accès aux informations renseignées sur la plateforme ROGER sont soumises à une obligation de confidentialité renforcée et ne peuvent notamment utiliser ces informations à toute autre fin. Ces personnes, appelés « référents », ont signé un engagement de confidentialité en vigueur pendant toute la durée de leurs attributions et demeurant effectif, sans limitation de durée après la cessation de leurs fonctions. Ils engagent également leur responsabilité pénale personnelle en cas de non-respect de cet engagement.

La plateforme est hébergée auprès d'un prestataire externe, en dehors des systèmes d'information d'OVHcloud.

7. Quels est le processus pour déclarer un signalement sur ROGER ?

La déclaration s'effectue en 4 étapes via la plateforme Roger. Tout d'abord, vous devez vous connecter à [go/roger](https://go.roger.ovh) ou sur www.roger.ovh. Sur cette page, il suffit de cliquer sur « Faire un nouveau signalement », suivre l'étape d'initialisation du signalement en choisissant la catégorie de l'alerte, renseigner les informations de contact (s'il ne s'agit pas d'un signalement anonyme) puis décrire les faits et le finaliser en validant et transmettant le signalement aux référents du dispositif.

Le lanceur d'alerte recevra un code confidentiel et personnel lui permettant depuis la page ROGER d'accéder à son signalement et d'échanger des messages privés et confidentiel avec les référents. [Rubrique « Accéder à un signalement existant »]

NB : Pour en savoir plus, vous pouvez retrouver le processus complet sur la page générale de la plateforme ROGER.

8. Puis-je garder l'anonymat lors de ma déclaration ?

Il est tout à fait possible de garder l'anonymat lors de votre déclaration, elle se fait lors de la phase d'identification du déclarant en cochant la case « Garder l'anonymat », aucune donnée d'identification n'est donc requise, vous pouvez toutefois en fin de signalement renseigner votre email pour recevoir une copie et être notifié(e) des évolutions de votre signalement. Dans le cadre d'un signalement anonyme, nous pouvons rencontrer des difficultés pour traiter au mieux votre signalement et pourrions être amenés à vous demander des éléments complémentaires lors de nos investigations.

9. Les signalements anonymes sont-ils traités différemment ?

Non, chaque signalement est traité de la même manière en suivant le même processus de recueil et traitement d'un signalement. (Cf. Question 10).

10. Après la déclaration de mon signalement, comment est-il recueilli et traité ?

Tout d'abord, les référents accusent réception du signalement. Celui-ci passe ensuite par 3 étapes clés :

- La recevabilité du signalement [durée de 2 semaines maximum],
- Le traitement du signalement [durée de 2 mois maximum].
- Si la violation est avérée, les référents rentreront dans la dernière phase de déploiement du plan d'actions.

NB : Pour en savoir plus, vous pouvez retrouver le processus complet sur la page générale de la plateforme ROGER.

11. Quelles sont mes mesures de protection en devenant lanceur d'alerte ? Suis-je protégé des mesures de représailles ?

Aucune mesure disciplinaire ou discriminatoire ne doit être exercée à l'encontre des collaborateurs signalant une alerte, même si les faits rapportés se révèlent infondés, sous réserve que les collaborateurs aient agi de bonne foi.

OVHcloud s'interdit de prendre des mesures de représailles, directe ou indirecte à l'encontre d'un collaborateur qui aurait signalé une alerte. Le non-respect de cet engagement donnera lieu à des sanctions disciplinaires pouvant aller jusqu'à la rupture du contrat de travail, conformément au droit applicable.

12. La ou les personnes faisant l'objet de mon signalement sera(ont)-t-elle(s) informées des faits qui lui/leurs sont reprochés ?

Oui, les principes du contradictoire et de la présomption d'innocence doivent être respectés et par conséquent chaque mise en cause identifiée lors de votre signalement sera informée des faits. Cette information est transmise à la suite des conclusions de l'enquête et au moment opportun par les référents.

13. Serai-je tenu au courant des conclusions de l'enquête ?

Oui, chaque lanceur d'alerte reçoit un retour synthétique des conclusions du signalement via les référents par le canal de la messagerie Roger, il est donc important de s'y rendre régulièrement pour se tenir informé des avancées du signalement.

14. Quelle est la durée de conservation des informations ?

La durée de conservation des informations est de 100 jours après la clôture du signalement.

15. Que se passe-t-il en cas de fausses déclarations ?

S'il apparaît à l'issue des investigations que le signalement réalisé par le lanceur d'alerte était réalisé de mauvaise foi ou encore pour porter atteinte à la réputation d'un tiers, un tel comportement pourra faire l'objet de sanctions disciplinaires ou encore de poursuites judiciaires par la personne visée par ces fausses allégations.

16. Que se passe-t-il si je vous fais part d'une préoccupation de bonne foi mais qu'il s'avère par la suite que je me suis trompé ?

Si au moment où vous avez donné les informations vous pensiez qu'elles étaient honnêtes, sincères et exactes, il n'y aura aucune répercussion négative. Bien entendu, si vous réalisez après avoir fait part de votre préoccupation que vous vous étiez trompé, merci d'en informer immédiatement les référents via la messagerie Roger.

17. ROGER est-il le seul canal pour ce genre de remontée ?

Non, c'est un des moyens pour remonter votre signalement. Vous pouvez également en parler directement avec le Chief Compliance Officer, votre supérieur hiérarchique, votre HRBP ou par les représentants du personnel le cas échéant.

