



Data privacy statement: Zurich Ethics Line

La présente mention d'information de confidentialité décrit les catégories d'informations collectées par Zurich Insurance Company Ltd et les filiales concernées (« nous », « notre/nos ») via la Zurich Ethics Line (« plateforme ») et la façon dont ces données sont traitées.

Nous prenons la protection des données très au sérieux et nous tenons à toujours rester transparents. Veuillez lire attentivement la présente mention d'information de confidentialité car elle contient des informations importantes concernant le traitement de vos données personnelles.

Lorsque vous soumettez une question ou un signalement via la Zurich Ethics Line, elle/il peut être accessible, à la demande des services Compliance, RH et Legal, aux niveaux local, régional ou du Groupe, afin de garantir le caractère responsable du signalement et son traitement conforme. Si vous ne souhaitez pas que votre signalement soit visible en dehors de votre pays, veuillez contacter directement votre responsable Compliance ou Legal local et aborder la question avec lui avant de soumettre un signalement sur cette plateforme.

En soumettant votre question ou votre signalement, vous acceptez que nous partagions votre question, votre signalement, ou vos données personnelles (le cas échéant et à moins que vous ne le signaliez de manière anonyme), avec d'autres membres du Groupe (très probablement avec un comité de triage basé en Amérique du Nord (États-Unis)) sur la base du besoin d'en connaître.

Dernière mise à jour en janvier 2025

Responsables de traitement des données et coordonnées :

Zurich Insurance Company Ltd, Mythenquai 2, 8002 Zurich, Suisse, et les filiales avec lesquelles vous interagissez agissent en qualité de responsables de traitement conjoints dans le cadre de cette plateforme.

Pour toute suggestion ou question concernant la protection des données sur cette plateforme, veuillez contacter l'équipe Protection des données de la filiale concernée ou nous envoyer un e-mail à l'adresse privacy@zurich.com.

Vous trouverez ici [des](#) informations supplémentaires sur la protection des données locales.

Quelles catégories de données peuvent-être collectées et traitées ?

On entend par « donnée personnelle » toute information associée à une personne identifiée ou identifiable.

Voici les données personnelles, communiquées lors de la soumission/l'actualisation d'un signalement ou d'une question, qui sont susceptibles d'être enregistrées par cette plateforme :

- votre nom et vos coordonnées (à moins que votre signalement soit anonyme) et si vous êtes employé.e par l'entreprise ;
- les noms et autres données d'identification des personnes que vous citez dans votre signalement/question le cas échéant (par ex. description des fonctions et coordonnées) et
- une description de la question ou de l'allégation, ainsi qu'une description des circonstances de l'incident.

Dans certains pays, la loi interdit les signalements sous couvert de l'anonymat. Néanmoins, vos données personnelles seront traitées en toute confidentialité et seront divulguées uniquement dans le respect de la présente mention d'information de confidentialité.

À quelles fins traitons-nous vos données personnelles ?

Nous traitons vos données personnelles pour pouvoir recevoir, clarifier et résoudre les allégations et questions relatives à l'éthique et à la conformité de manière cohérente au sein du Groupe.

Sur quelles bases légales traitons-nous vos données personnelles ?

Nous traitons vos données personnelles dans notre intérêt légitime en vue de contrôler la conformité avec les lois, les réglementations, les politiques internes et notre Code de conduite de manière cohérente au sein du Groupe.

Dans les pays où la réglementation impose des systèmes d'alerte, notre fondement légal est de respecter une obligation légale.

Comment les données personnelles seront-elles traitées après votre signalement et qui peut accéder à vos données personnelles ?

En vue de traiter et de clarifier votre signalement et sous réserve des dispositions légales en vigueur, il se peut que les données personnelles que vous communiquez soient consultées, traitées et utilisées, uniquement en cas de nécessité absolue et avec notre consentement écrit, par le personnel qualifié de notre entreprise, des conseillers externes (par ex. avocats), ou, dans certains cas limités, par le personnel technique de GCS Compliance Services Europe Ltd. Co., exerçant sous le nom de NAVEX Global, (« NAVEX »), afin d'apporter un soutien technique.

Les données personnelles que vous communiquez peuvent également être divulguées en cas de nécessité absolue à des autorités administratives ou judiciaires spécifiques afin de se conformer à des exigences légales ou réglementaires, par ex. réglementation relative à la lutte contre le blanchiment d'argent, ou bien si nous pensons que leur divulgation est raisonnablement nécessaire pour nous protéger contre des fraudes, protéger nos actifs ou d'autres droits ou ceux d'autres utilisateurs de la plateforme, de tiers, ou du public en général.

Stockage des données

Nous utilisons NAVEX pour stocker les données personnelles dans des bases de données situées sur des serveurs à Francfort (Allemagne) et à Amsterdam (Pays-Bas).

NAVEX interdit l'accès à ou l'utilisation non autorisé(e) des informations personnelles stockées sur ses serveurs. Ce type d'accès constitue une violation de la loi et NAVEX effectuera des enquêtes approfondies et prendra les mesures juridiques nécessaires contre toute personne ayant accédé illégalement aux informations contenues dans ses systèmes.

Vos données personnelles sont-elles en sécurité ?

Nous appliquons des mesures techniques et organisationnelles strictes pour protéger vos données personnelles contre l'accès par des personnes non autorisées et contre tout traitement illégal, toute perte accidentelle, toute destruction et tout dommage, en ligne et hors ligne.

Ces mesures comprennent :

- la formation du personnel concerné pour que celui-ci connaisse nos obligations en matière de protection des données lorsqu'il traite des données personnelles ;
- des contrôles administratifs et techniques afin de limiter l'accès aux données personnelles aux cas de nécessité absolue (procédures d'attribution de rôles et de droits, mots de passe) ;
- des mesures de sécurité techniques (y compris pare-feux, cryptage et logiciels antivirus, surveillance des accès, contrôles spécifiques au client, examens réguliers des comptes d'utilisateurs, sauvegardes régulières, etc.) ;
- la gestion des incidents (procédures rigoureuses en cas d'incidents, résolution des erreurs, incidents et fuites de données personnelles, etc.) ;
- des mesures de sécurité physiques, telles que des badges de sécurité destinés au personnel pour accéder à nos locaux.

Malgré l'application de mesures de sécurité strictes après avoir reçu vos données personnelles, la transmission de données n'est jamais totalement sécurisée – en particulier sur Internet. C'est pourquoi nous ne pouvons garantir une sécurité absolue des données qui nous sont transmises ou que nous transmettons.

NAVEX applique des mesures administratives, physiques et technologiques reconnues dans le secteur afin de protéger les données personnelles contenues dans ses systèmes contre toute perte, toute utilisation abusive, tout accès non autorisé et toute altération. NAVEX assure que tous les collaborateurs, contractants, sociétés, organismes ou fournisseurs ayant accès aux données personnelles contenues dans ses systèmes sont soumis aux obligations légales et professionnelles de protéger ces données personnelles. Consultez la notice d'information de confidentialité de NAVEX [ici](#).

Transferts transfrontaliers

NAVEX a son siège social au Royaume-Uni.

Nous avons des entités juridiques dans les régions APAC, EMEA, LATAM et NA. Il est donc possible que des signalements proviennent de ces régions ou que des données personnelles soit transférées à des destinataires dans ces pays. Les droits d'accès des utilisateurs sont configurés de sorte à éviter tout transfert de données



personnelles en provenance de l'Espace économique européen, du Royaume-Uni ou de la Suisse en dehors de ces mêmes régions.

En ce qui concerne Zurich Cover More, une exception à cet accès général des utilisateurs s'applique afin d'évaluer de manière cohérente les questions ou les rapports concernant l'éthique et la conformité au sein du Groupe par un comité de triage basé en Amérique du Nord (États-Unis).

Combien de temps conservons-nous vos données personnelles ?

Nous conservons les données personnelles que vous nous communiquez autant de temps que l'impose le traitement de votre signalement ou, le cas échéant, le temps nécessaire pour engager des sanctions ou satisfaire à des exigences légales ou financières. Si des procédures judiciaires ou disciplinaires sont engagées, nous conservons vos données personnelles jusqu'à ce que ces procédures soient définitivement closes. Nous conservons les données personnelles dans la mesure autorisée par la loi et nos politiques en matière de conservation. Autrement, nous supprimons ou rendons anonymes les données personnelles dont nous n'avons plus besoin, dans la mesure autorisée par la loi.

Vos droits

Vous avez différents droits dont nous souhaiterions vous informer : le droit d'accéder à vos données personnelles, le droit de rectifier vos données (si elles sont inexactes), le droit de demander l'effacement de vos données (si leur conservation n'est plus nécessaire aux fins du traitement envisagées), le droit de limiter le traitement de vos données (par ex. si vous contestez l'exactitude de vos données personnelles que nous traitons), le droit à la portabilité de vos données dans certaines circonstances et le droit de déposer une plainte auprès de l'autorité de contrôle compétente.

Si vous souhaitez exercer vos droits mentionnés ci-dessus, veuillez contacter l'équipe locale chargée de la protection de la vie privée des filiales respectives ou nous contacter par e-mail à l'adresse suivante privacy@zurich.com.

Toute enquête en cours est susceptible de limiter les droits susmentionnés ou de vous en priver. Si l'un des droits précités est limité ou refusé, il convient d'en fournir les motifs avec des documents à l'appui. Lorsque l'accès aux données personnelles d'un individu concerné est autorisé, les données personnelles des malfaiteurs présumés ou de tiers (par ex. informateurs, dénonciateurs ou témoins) peuvent être supprimées des documents, excepté dans certains cas exceptionnels.