DEMANDE SIGNALEUR DE CONFIANCE LISTE DE DOCUMENTS JUSTIFICATIFS

Le présent document décrit le type de documentation et d'informations que les demandeurs du statut de signaleurs de confiance, au sens de l'article 22 du DSA, peuvent joindre à leur demande. À cet égard, une distinction est faite entre la documentation plus essentielle et les pièces justificatives complémentaires qui peuvent renforcer davantage la candidature.

Si l'information est accessible au public, un lien renvoyant au site Internet peut suffire. Les informations peuvent également être fournies sous forme groupée plutôt que dans des documents séparés.

Si vous fournissez un document contenant des informations que vous estimez confidentielles, veuillez également fournir une version non confidentielle de ce document en même temps. Dans la version confidentielle, les passages confidentiels doivent être clairement indiqués dans le texte.

1. Recevabilité de la candidature

Preuve que le candidat possède une personnalité juridique et n'est pas une personne physique (les particuliers sont exclus), et que le candidat est établi en Belgique.

1. Acte constitutif et/ou statuts ;
2. Données d'entreprise (telles que le numéro d'entreprise auprès de la Banque-Carrefour des Entreprises, le lieu d'établissement, etc.) ;
3. Mandat de représentation ou déclaration sur l'honneur comme preuve de mandat valide pour lier l'entité, si cela ne ressort pas des statuts.

2. Informations générales/mission (déclaration)

1. Déclaration de mission (éventuellement tirée des statuts) ;
2. Le cas échéant : conditions générales de l'entité ;
3. Si le signalement est une nouvelle activité pour l'entité : description de la motivation ou de l'importance de devenir un signaleur de confiance.

3. Expertise et compétences particulières aux fins de détecter, d'identifier et de notifier des contenus illicites

3.1 De l'entité en général

1. Preuve d'un domaine d'expertise désigné et des connaissances linguistiques nécessaires ;
2. Le cas échéant : preuve d'une coopération (antérieure) en tant que signaleur avec une ou plusieurs fournisseur(s) de plateforme(s) en ligne avant l'existence du DSA, y compris l'accord avec ce ou ces fournisseur(s) de cette ou ces plateforme(s) en ligne ;
3. Description des processus, procédures ou stratégies utilisés pour faire des notifications (par ex., modus operandi, flow chart, etc.) ;

4. Utilisation d'outils (programmes informatiques, outils de détection/surveillance des contenus illicites, détection de tendances, outils garantissant le traitement sécurisé des informations, notamment les contenus illicites et les données à caractère personnel, autres mécanismes…) ;
5. Matériel de formation pour le personnel : preuve de formation à l'identification de contenus illicites, la connaissance des normes juridiques pertinentes (par exemple, DSA, droit national), l'évaluation des notifications…

Documentation complémentaire :

6. Publications : études, rapports annuels, avis, recommandations présentant des notifications relatives aux plateformes en ligne, etc. ;
7. Exemples anonymisés de notifications précédentes, exemples de rapports soumis à des plateformes en ligne ou à des autorités ;
8. Preuve d'adhésion/de coopération avec des organismes ou des réseaux d'experts tels que INHOPE, Europol, unités de lutte contre la cybercriminalité, réseaux indépendants de fact-checking, EU Internet Forum ;
9. Politique ou procédures de recrutement et de sélection des personnes qui effectueront les activités de signalement et, une fois en service, leur évaluation et suivi ;
10. Autres données qui démontrent une expérience antérieure en matière de détection, d'identification et/ou de notification de contenus illicites.

3.2 De l'équipe qui effectuera la tâche de signaleur de confiance

1. Présentation/organigramme de la structure/l'organisation de l'équipe (par ex., taille de l'équipe, nombre d'équivalents temps plein actifs, bénévoles, etc.) ;
2. Profils, CV des membres du personnel concernés, y compris les formations spécifiques et les diplômes dans le domaine d'expertise spécifique.

Documentation complémentaire :

3. Certificats obtenus ou formations spécifiques suivies : par ex. certificat juridique/de conformité en modération de contenu, protection des données, droit numérique, cybersécurité, sécurité numérique, programmes de politique de contenu suivis sur les plateformes en ligne, etc. ;
4. Contributions fournies par ces personnes dans les domaines d'expertise dans les études, forums, séminaires, workshops, etc. ;
5. Informations sur l'espace de bureau adapté, les capacités de télétravail.

4. Indépendance vis-à-vis des fournisseurs de plateformes en ligne

4.1 Organisation

1. Organigramme des organes décisionnels de l'entité et, dans le cas d'un groupe d'entreprises, illustration schématique de la structure du groupe ;
2. Description des membres du conseil d'administration, des actionnaires ou des membres de l'association (avec ou sans contrôle, y compris leurs relations, telles que définies dans un éventuel accord d'actionnaires ou de parties prenantes). Il convient d'indiquer pour toutes les personnes concernées – membres, actionnaires et administrateurs – leurs intérêts ou leur participation dans un ou des fournisseur(s) de plateformes en ligne le cas échéant ;

3. Règles de prise de décision (règlement interne, droit de vote, etc.) et description du processus de prise de décision pour les activités de signalement, ainsi que les documents démontrant l'indépendance de l'entité et du personnel vis-à-vis des plateformes en ligne et l'impartialité lors de la prise de décision ;
4. Règlement interne ou règles de procédure en cas de conflits d'intérêts, ou code éthique ;
5. Description des contrats et partenariats conclus avec un ou des fournisseur(s) de plateformes en ligne, y compris une déclaration d'indépendance.

Documentation complémentaire :

6. Recherche indépendante ou recommandation de politique générale permettant de déduire qu'il n'y a aucune influence exercée par le ou les fournisseur(s) de plateformes en ligne.

4.2 Financier

1. Comptes annuels, au moins pour les deux dernières années ;
2. S'il s'agit d'une entité nouvellement créée : plan d'activités financières ou plan budgétaire ;
3. Description de toutes les sources de financement (subventions, dons, cotisations des adhérents, etc.) ;
4. Le cas échéant : accords avec des partenaires, sponsors et/ou investisseurs, y compris une description des engagements financiers, montrant que leur soutien (financier) n'affecte pas la politique ou les décisions (s'il y a des clauses de confidentialité, à partager à titre confidentiel).

Documentation complémentaire :

5. Le cas échéant : audit externe confirmant l'indépendance financière ;
6. Description de la manière dont le candidat rend publics ses rapports de financement (par ex., un lien vers la publication sur son site Internet).

5. Diligence, précision et objectivité

1. Procédures, mécanismes ou lignes directrices internes démontrant comment les contenus illicites sont identifiés et signalés avec précision (par ex., contrôles ou vérifications réalisés pour effectuer la notification), et décrivant la méthodologie utilisée pour une évaluation objective ;
2. Mécanisme de correction et de révision permettant d'apporter des ajustements lorsque les protocoles de signalement ne sont pas réalisés correctement (par ex., un système de double vérification) ;
3. Description des outils manuels et/ou automatisés utilisés pour identifier et vérifier les contenus illicites ;
4. Fournir tous les détails concernant les relations commerciales, financières et/ou institutionnelles que l'entité entretient avec l'État et les personnes et partis politiques, et indiquer comment l'entité assure, dans de telles relations, l'indépendance de l'activité de signalement ;
5. Preuve de politique de stockage et de protection des données sécurisées, et de conformité avec le RGPD.

Documentation complémentaire :

6. Preuve de cas antérieurs où des notifications ont été réexaminées et des corrections ont été apportées ;

7. Processus permettant aux plateformes en ligne de notifier au signaleur de confiance toute notification qu'elles jugent erronée, injustifiée ou incomplète ;
8. Tout rapport annuel ou autre type de rapport indiquant le nombre de notifications (y compris le pourcentage de notifications correctes et abusives, les ajustements, l'aperçu des rapports contestés et leur traitement, les conclusions, les recommandations, etc.) ;
9. Rapports ou descriptions des activités ou campagnes précédentes relatives à la modération de contenu, la protection des utilisateurs, la sécurité en ligne, etc.

6. Obligation d'information

Les signaleurs de confiance reconnus doivent publier au moins une fois par an un rapport facile à comprendre et détaillé.

Les documents suivants peuvent être fournis à titre complémentaire :

1. Procédure d'élaboration du rapport annuel, reprenant notamment la personne responsable de la collecte et de l'analyse des données ;
2. Description des chiffres et/ou statistiques utilisés pour collecter les données et ensuite transposés dans le rapport annuel (y compris le nombre de notifications erronées) ;
3. Explication de la manière dont les données sont stockées, conformément aux règles du RGPD et sans inclure de données à caractère personnel dans le rapport ;
4. Autres rapports similaires ;
5. Description des moyens techniques ou des systèmes de rapportage.

ANNEXE – Liste de domaines de contenu illicite

La présente liste n'est pas exhaustive et est purement indicative. Elle reflète les domaines potentiels de contenu illicite dans les États membres qui pourraient constituer des domaines d'expertise pour les entités candidates au statut de signaleur de confiance.

- **Délits concernant les animaux**
  - Maltraitance animale
  - Vente illégale d'animaux et/ou trafic d'espèces sauvages
  - Autres
- **Protection des données et violations de la vie privée**
  - Violation des données biométriques
  - Absence de motif de traitement des données
  - Atteintes au droit à l'oubli
  - Falsification des données
  - Autres violations des données relatives au RGPD
  - Autres
- **Discours illégal***
  - Diffamation
  - Discrimination
  - Discours haineux
  - Menaces de violence (comme des menaces de mort)
  - Négation de l'Holocauste
  - Autres
- **Atteintes à la propriété intellectuelle et à d'autres droits commerciaux**
  - Atteintes au droit d'auteur
  - Contrefaçon de dessins ou modèles
  - Atteintes aux droits sur des manifestations sportives
  - Atteintes aux indications géographiques
  - Atteintes aux brevets
  - Violation des secrets commerciaux
  - Atteinte aux marques
  - Produits de contrefaçon
  - Autres
- **Effet négatif sur le discours civique et les processus électoraux**
  - Activités de manipulation de l'information et d'ingérence menées depuis l'étranger
  - Manipulations des informations visant à affecter l'authenticité/le résultat des élections
  - Autres
- **Comportement non consenti**
  - Partage non consenti d'images
  - Partage non consenti de matériel créé à l'aide de technologies d'hypertrucage (deepfake) ou de technologies similaires et utilisant des caractéristiques d'un tiers
  - Doxing (divulgation d'informations personnelles concernant une personne)
  - Autres
- **Brimades/intimidation en ligne**
  - Traque furtive (stalking)
  - Harcèlement sexuel
  - Autres
- **Pornographie ou contenus à caractère sexuel**
  - Images d'abus sexuels (à l'exclusion des contenus représentant des mineurs)
  - Viol et autres violences sexuelles (représentation du viol et incitation au viol)
  - Autres

* *Y compris tous types de discours haineux publics, quel que soit le support et le contenu (à savoir des images, des vidéos, des textes, des déclarations publiques, etc.).*

• **Délits envers les mineurs** ○ Échec de la mise en œuvre de restrictions liées à l'âge concernant les mineurs ○ Contenus représentant des abus sexuels commis sur des enfants ○ Approche (grooming) ou sollicitation de mineurs à des fins sexuelles ○ Défis dangereux ○ Autres • **Risque pour la sécurité publique** ○ Provocation à commettre un délit dangereux pour la sécurité publique ○ Organisations illégales ○ Risque de dommages environnementaux ○ Risque pour la santé publique ○ Contenu à caractère terroriste ○ Autres • **Escroqueries et/ou fraudes** ○ Comptes non authentiques ○ Annonces non authentiques ○ Avis d'utilisateur non authentiques ○ Imposture ou piratage de compte ○ Hameçonnage ○ Systèmes de vente pyramidale ○ Autres	• **Incitation à l'autodestruction** ○ Contenus promouvant les troubles de l'alimentation ○ Incitation à l'automutilation ○ Incitation au suicide ○ Autres • **Étendue illégale de l'accès à la plateforme/au contenu** ○ Échec de la mise en œuvre de restrictions d'âge autres que celles concernant les mineurs ○ Exigences géographiques illégales ○ Non-respect des exigences linguistiques Autres restrictions d'accès discriminatoires ○ Autres • **Produits dangereux et/ou illégaux** ○ Informations insuffisantes sur les professionnels ○ Offre illégale de biens et services régulés (par ex. santé) ○ Vente de produits non conformes (par ex. jouets dangereux) ○ Trafic d'armes et de drogues illicites ○ Pratiques illégales selon la législation en matière de protection des consommateurs ○ Malware et ransomware ○ Autres • **Violence** ○ Actions néfastes coordonnées ○ Violence fondée sur le genre ○ Exploitation des êtres humains ○ Traite des êtres humains ○ Autres