Checklist de la directive européenne des lanceurs d'alerte

Déterminez les conditions requises dans votre entreprise ou organisation pour la mise en place réussie d'un système interne de recueil et de traitement d'alerte

- [ ] Le système peut-il garantir la confidentialité absolue du lanceur d'alerte afin qu'il n'ait pas à craindre de représailles ?
- [ ] Le fournisseur peut-il prouver que ni lui ni des tiers n'ont accès au contenu sensible des alertes ?
- [ ] Les employés du monde entier peuvent-ils soumettre des alertes en toute sécurité 24 heures sur 24 et 7 jours sur 7 ?
- [ ] Les ressources internes qui permettent la mise en œuvre de la protection des données et de la sécurité informatique sont-elles suffisantes ?
- [ ] Le système est-il certifié conforme au droit européen (RGPD) ?
- [ ] Le système peut-il être adapté de manière flexible aux besoins spécifiques de votre entreprise, par exemple grâce à l'authentification unique (SSO) ?
- [ ] Les serveurs sont-ils situés dans un data center de haute sécurité en Europe ?
- [ ] Le système est-il facile à gérer, même avec un petit nombre d'employés ?
- [ ] Les coûts de votre système de recueil d'alerte peuvent-ils être représentés de manière transparente sous la forme d'un modèle de coût global, vous offrant ainsi la sécurité nécessaire en matière de planification ?
- [ ] Les alertes et leurs mesures de suivi peuvent-elles être documentées de façon infalsifiable ?

Êtes-vous soutenu et conseillé lors de la mise en œuvre ?

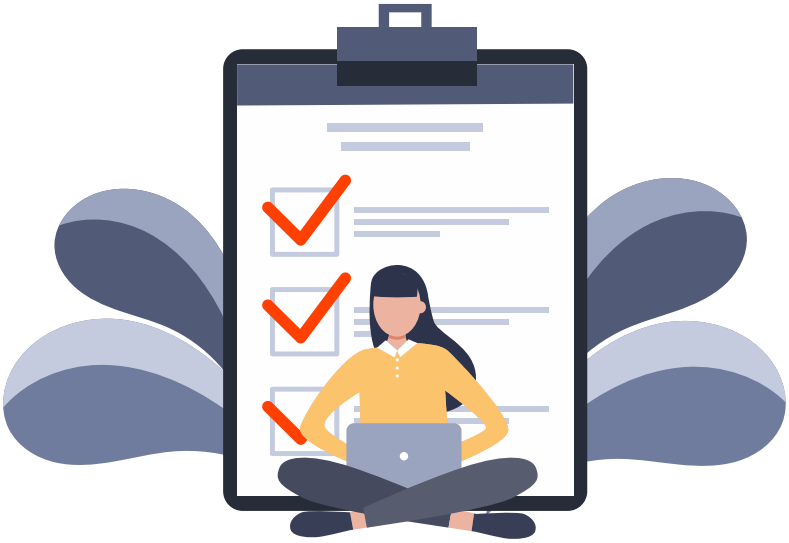
- [ ] Le Key Account Management dédié est-il fiable et expérimenté et en mesure de vous fournir les bonnes pratiques et l'expertise nécessaire ?

- [ ] Recevez-vous une aide supplémentaire sur des sujets comme la protection des données, la sécurité de l'information, la communication avec les représentants du personnel et les questions relatives aux comités d'entreprise ?

- [ ] Vous offre-t-on des avantages supplémentaires comme la participation à des événements, des séminaires, la mise en réseau avec des experts et avec une communauté dédiée à la conformité ?

Créer les conditions nécessaires à la réussite de votre projet et communiquer avec les acteurs clés.

- [ ] Les pratiques utilisées pour informer et promouvoir une culture d'entreprise intègre et éthique sont-elles transmises à vos employés ?



EQS Integrity Line répond à toutes les exigences de la directive européenne sur la protection des lanceurs d'alerte

Prescriptions de la directive	Mise en œuvre d'EQS Integrity Line
Obligation de conception de canaux de signalement internes pour la réception des signalements et leur suivi (art. 8 al. I, IX)	Soumission d'alertes écrites
	Soumission d'alertes par téléphone
	Coordination des mesures de suivi
Alerte écrite, orale ou sous les deux formes (art. 9 al. II)	Disponible en continu et dans le monde entier
	Soumission d'alertes dans plus de 70 langues
	Enregistrement sonore avec distorsion de la voix
	Le lanceur d'alerte est informé avant l'enregistrement
	Confiance grâce au traitement transparent des données vis-à-vis des lanceurs d'alerte
Garantie de la confidentialité de l'identité du lanceur d'alerte et de la personne concernée (art. 9 al. I a, art. 16 al. I)	Sécurité d'accès éprouvée (sécurité informatique maximale, logarithmes de chiffrement modernes, data center de données haute sécurité)
Obligation de confidentialité	Certification ISO 27001
	Principe flexible à base de droits et de rôles
	Pseudonymisation/anonymisation en conformité avec la protection des données
	Recommandations pour les lanceurs d'alerte afin de préserver l'anonymat

Accusé de réception de l'alerte et retour d'information en temps utile (art. 9 al. I b et f)	Communication sécurisée grâce à une boîte de dialogue protégée Les modules de texte facilitent la confirmation de la réception et le retour d'information aux lanceurs d'alerte Nouvelles soumissions pour respecter les délais
Traitement des données à caractère personnel conformément au RGPD de l'UE et à la directive précédente (art. 17) **Pas de collecte de données non pertinentes ou effacement immédiat**	Premier système de recueil d'alerte certifié en matière de protection des données (RGPD de l'UE) Adaptable à une éventuelle situation juridique spécifique à un pays Préréglages conformes à la protection des données pouvant être prouvés Les catégories d'alertes et les questions prédéfinies empêchent la collecte de données non pertinentes
Documentation de toutes les alertes reçues conformément aux obligations de confidentialité (art. 18) **Conservation jusqu'à ce que les exigences de la directive/du droit de l'Union/du droit national soient remplies** **Vérification, correction et confirmation de la transcription d'une alerte téléphonique**	Documentation infalsifiable Efficacité mesurable grâce à des rapports de gestion performants Peut être archivé indéfiniment après anonymisation Vérification, correction et confirmation grâce au dialogue avec le lanceur d'alerte

Vous souhaitez proposer un système de recueil et de traitement d'alerte dans votre entreprise pour respecter la directive européenne des lanceurs d'alerte ?

EQS Integrity Line est la ligne d'alerte la plus utilisée en Europe et nous disposons de plus de 1 600 clients dans le monde. Le dispositif d'alerte interne est sécurisé et anonyme. Il permet à vos employés de signaler des actes répréhensibles tels que la corruption, les abus de pouvoir, la discrimination et le harcèlement en interne avant de contacter les autorités ou les médias.

Obtenez votre démo personnelle →

Plus de 1 600 entreprises dans le monde font confiance au dispositif d'alerte numérique EQS Integrity Line.

ACCORINVEST

KEYRUS

KILOUTOU

RAJA
N°1 EUROPÉEN DE L'EMBALLAGE

TOSHIBA

Worldline

EQS GROUP

EQS Group SAS | 3 Rue Tronchet | 75008 Paris
Tel.: +33 1 43148510

www.integrityline.com