



Politique de gestion des données

Responsable de la politique : Responsable informatique et sécurité

Date d'entrée en vigueur : 22 février 2024

Visée

Garantir que les informations soient classées, protégées, conservées et éliminées de manière sécurisée selon leur importance pour l'entreprise.

Champ d'application

L'ensemble des données, informations et systèmes d'information de Evalandgo Software.

Politique

Evalandgo Software classe les données et les systèmes d'information conformément aux exigences légales, à leur sensibilité et à leur importance pour ses activités de manière à garantir que lesdites informations fassent l'objet d'un niveau de protection approprié. Il revient aux propriétaires des données d'identifier toute exigence supplémentaire applicable à certaines données ou toute exception aux exigences de traitement standard.

Les systèmes d'information et les applications sont classés en fonction de la plus haute classification des données qu'ils stockent ou traitent.

Classification des données

Afin d'aider Evalandgo Software et ses employés à identifier facilement les exigences associées à différents types d'informations, l'entreprise a défini trois classes de données.

Données confidentielles

Données hautement sensibles nécessitant les niveaux de protection les plus élevés. L'accès est limité à des employés ou à des services spécifiques, et les données ne peuvent être transmises à autrui qu'avec l'approbation du propriétaire des données ou d'un dirigeant de l'entreprise. Ces données incluent :

- Les données clients
- Les données à caractère personnel
- Les données financières et bancaires de l'entreprise
- Les informations sur le salaire, la rémunération et la paie
- Les plans stratégiques
- Les rapports d'incident
- Les rapports d'évaluation des risques
- Les rapports sur les vulnérabilités techniques

- Les informations d'authentification
- Les secrets et clés privées
- Le code source
- Les données sur les litiges

Données restreintes

Les informations propriétaires de Evalandgo Software qui nécessitent une protection renforcée. L'accès est restreint aux seuls employés directement concernés, en fonction des besoins de l'entreprise. La transmission de ces données à des intervenants extérieurs à l'entreprise doit faire l'objet d'une autorisation. Par défaut, cela concerne toutes les informations relatives à l'entreprise, sauf indication contraire. Voici quelques exemples :

- Politiques internes
- Documents juridiques
- Comptes-rendus de réunions et présentations internes
- Contrats
- Rapports internes
- Messages Google Chat
- E-mails

Données publiques

Documents destinés au public pouvant être librement diffusés en dehors de Evalandgo Software. Exemples :

- Documents marketing
- Descriptions de produits
- Notes de publication
- Politiques externes

Étiquetage

Les données confidentielles doivent porter la mention « confidentiel » lorsque des copies papier sont produites en vue d'être distribuées.

Gestion des données

Gestion des données confidentielles

Les données confidentielles sont soumises aux exigences suivantes en matière de protection et de traitement :

- L'accès est restreint à des employés, des rôles et/ou des services spécifiques
- Les systèmes confidentiels doivent rendre impossible tout accès non authentifié ou anonyme
- Les données confidentielles de clients ne doivent pas être utilisées ou stockées dans des systèmes/environnements hors production
- Les données confidentielles doivent être chiffrées lorsqu'elles sont statiques et en transit sur les réseaux publics, conformément à la politique de cryptographie
- Les disques durs d'appareils mobiles contenant des données confidentielles, y compris les ordinateurs portables, doivent être chiffrés
- Les appareils mobiles stockant ou accédant à des données confidentielles doivent être protégés par un mot de passe de connexion (ou équivalent, tel que biométrie) ou un code

d'accès et doivent être configurés de manière à entraîner le verrouillage de l'écran après cinq (5) minutes de non-utilisation

- Les sauvegardes doivent être chiffrées
- Les données confidentielles ne doivent pas être stockées sur des téléphones, des appareils ou des supports amovibles personnels, y compris des clés USB, des CD ou des DVD
- Les documents papier doivent porter la mention « confidentiel » et être conservés et éliminés de manière sécurisée et approuvée, conformément aux politiques et procédures de traitement et de destruction des données
- Les documents papier ne doivent être créés qu'en fonction d'un besoin commercial et doivent être évités dans la mesure du possible
- Les disques durs et les appareils mobiles utilisés pour stocker des informations confidentielles doivent être nettoyés correctement avant d'être jetés ou détruits
- L'envoi de données confidentielles à des personnes ou entités extérieures à l'entreprise doit être régi par un contrat ou un arrangement légal et s'effectuer avec l'autorisation écrite explicite de la direction ou du propriétaire des données

Gestion des données restreintes

Les données restreintes sont soumises aux exigences suivantes en matière de protection et de traitement :

- L'accès est restreint aux seuls utilisateurs directement concernés, en fonction des besoins de l'entreprise
- Les systèmes restreints doivent rendre impossible tout accès non authentifié ou anonyme
- L'envoi de données restreintes à des personnes ou entités extérieures à l'entreprise ou à des utilisateurs autorisés doit faire l'objet d'une autorisation de la direction et être régi par un contrat ou un arrangement légal, ou s'effectuer avec l'autorisation du propriétaire des données
- Les documents papier doivent être conservés et éliminés de manière sécurisée et approuvée, conformément aux politiques et procédures de traitement et de destruction des données
- Les disques durs et les appareils mobiles utilisés pour stocker des informations restreintes doivent être nettoyés correctement avant d'être jetés ou détruits

Gestion des données publiques

Aucune mesure de protection ou de contrôle du traitement particulière n'est requise pour les données publiques. Ces données peuvent être distribuées librement.

Conservation des données

Evalandgo Software doit conserver les données tant que l'entreprise aura besoin de les utiliser, ou pour répondre aux exigences réglementaires ou contractuelles. Une fois que les données ne sont plus nécessaires à l'entreprise, celles-ci doivent être supprimées ou archivées de manière sécurisée. Les propriétaires des données, de concert avec un conseiller juridique, peuvent déterminer la durée de conservation applicable à leurs données.

Les données à caractère personnel doivent être supprimées ou anonymisées dès qu'elles n'auront plus d'usage commercial.

Les périodes de conservation sont documentées dans la matrice de conservation des données figurant à l'annexe B de la présente politique.

Élimination des données et des appareils

Les données restreintes ou confidentielles doivent être supprimées de manière sécurisée lorsqu'elles ne sont plus nécessaires à l'entreprise. Evalandgo Software doit évaluer les données et les pratiques d'élimination de ses fournisseurs tiers conformément à la politique de gestion des tiers. Seuls les tiers qui répondent aux exigences de Evalandgo Software en matière d'élimination sécurisée des données doivent être mobilisés pour le stockage et le traitement des données restreintes ou confidentielles.

Evalandgo Software doit veiller à ce que toutes les données restreintes et confidentielles soient supprimées de manière sécurisée des appareils de l'entreprise avant ou au moment de leur élimination.

Les documents papier confidentiels et restreints doivent être déchiquetés ou éliminés de toute autre manière à l'aide d'une méthode sécurisée.

Les données à caractère personnel ne doivent être collectées, utilisées et conservées que tant que l'entreprise poursuit un objectif commercial légitime. Les données à caractère personnel doivent être supprimées en toute sécurité et éliminées à la résiliation du contrat, conformément à la politique de l'entreprise, aux engagements contractuels et à toutes les lois et réglementations applicables. Les données à caractère personnel doivent également être supprimées en réponse à une demande vérifiée d'un consommateur ou d'une personne concernée, lorsque l'entreprise n'a pas d'intérêt commercial légitime ou d'autre obligation légale de conserver les données.

Examen annuel des données

La direction évaluera les exigences en matière de conservation des données au cours de l'examen annuel de la présente politique. Les données seront supprimées conformément à la présente politique.

Exigences légales

Dans certaines circonstances, Evalandgo Software peut faire l'objet de procédures judiciaires nécessitant la conservation de certaines données pour des raisons juridiques, suite à des poursuites judiciaires ou à d'autres questions, tel que stipulé par le conseiller juridique de Evalandgo Software. Ces données et informations sont exemptées de toute autre exigence spécifiée dans la présente Politique de gestion des données et doivent être conservées conformément aux exigences spécifiées par le Service juridique. Toutes ces retenues et exigences particulières de conservation font l'objet d'un examen annuel de concert avec le conseiller juridique de Evalandgo Software, en vue d'évaluer toute évolution des exigences et de leur portée.

Respect de la politique

Evalandgo Software évaluera et contrôlera la conformité à la présente politique par le biais de diverses méthodes, incluant sans s'y limiter des rapports d'outils professionnels et des audits internes et externes.

Exceptions

Les demandes d'exception à cette politique doivent être soumises à l'approbation du responsable informatique et sécurité.

Violations et application

Toute violation connue de cette politique doit être rapportée au responsable informatique et sécurité. Les violations de la présente politique sont susceptibles d'entraîner le retrait ou la suspension immédiats des privilèges sur le système et le réseau et/ou des mesures disciplinaires conformément aux procédures en place dans l'entreprise, y compris la résiliation du contrat de travail.

Version	Date	Description	Auteur	Approuvé par
1.0	22-Fev-2024	Première version	Valentin Boschattel	Valérie Marusiak

ANNEXE A - Procédure interne de conservation et d'élimination

L'équipe d'ingénierie de Evalandgo Software est chargée de définir et d'appliquer les procédures de conservation et d'élimination des données pour les comptes et les appareils gérés par Evalandgo Software.

Comptes clients :

1. Les comptes et les données des clients seront supprimés dans un délai de soixante (60) jours à compter de la résiliation du contrat par des procédés manuels de suppression des données.

Appareils :

1. Les appareils des employés seront rendus à l'entreprise dans les plus brefs délais suivant la résiliation du contrat. Les employés en télétravail recevront une étiquette d'expédition et il sera procédé au suivi du retour de leur appareil.
2. Les appareils rendus à l'entreprise pourront être effacés puis réaffectés ou retirés de l'inventaire ; Evalandgo Software effacera l'appareil de manière sécurisée lors de la réaffectation.
3. Les images des appareils pourront être conservées à la discrétion de la direction à des fins professionnelles

Destruction d'appareils ou de supports électroniques

Dans les cas où un appareil est endommagé de telle sorte que Evalandgo Software est dans l'incapacité d'accéder à la Partition de récupération pour effacer le disque, Evalandgo Software peut éventuellement décider d'utiliser un service de traitement des déchets électroniques incluant la destruction des données avec un certificat. Evalandgo Software conservera les certificats de destruction pendant un an. La destruction physique peut être facultative s'il est attesté que l'appareil est chiffré à l'aide d'un chiffrement de disque complet, prévenant tout risque de récupération des données.

La direction évaluera cette procédure au moins une fois par an.

ANNEXE B - Matrice de conservation des données

Système ou application	Description des données	Période de conservation
Produits SaaS (AWS) de Evalandgo Software	Données clients	Jusqu'à 60 jours après la résiliation du contrat
AutoSupport de Evalandgo	Instance client et métadonnées,	Indéterminée

