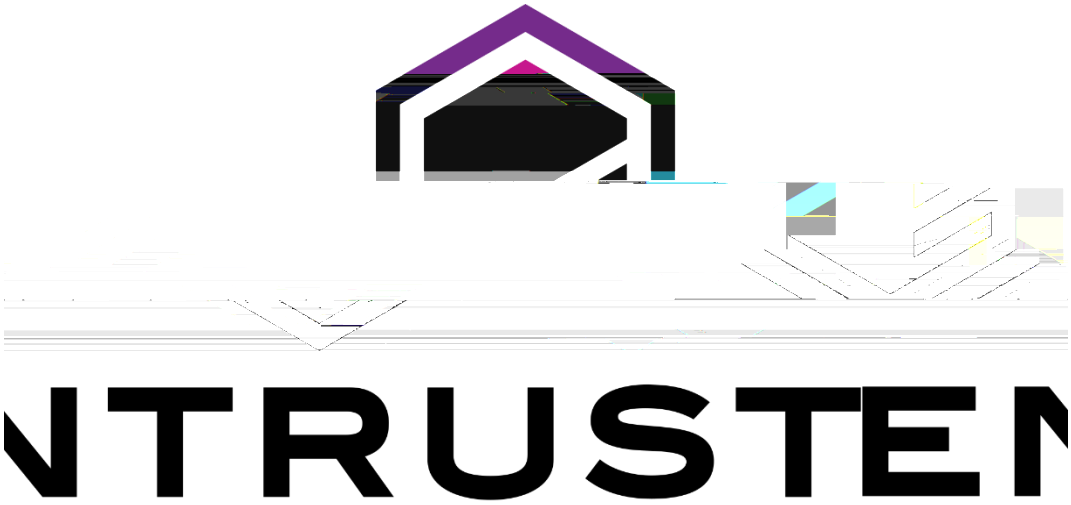

| | |
|---|---|
| Version du document | 1.6 |
| Date | 5 septembre 2023 |

12.1 Coordonnées de contact

## 1. introduction

Entrust Corporation et ses filiales et sociétés affiliées (collectivement, « Entrust » ou la « Société ») traitent les données personnelles de leurs collaborateurs, travailleurs intérimaires, partenaires, fournisseurs et clients en qualité de contrôleur de données, et les données personnelles de leurs clients et utilisateurs finaux en qualité de processeur de données. Lorsqu'Entrust traite des données personnelles, il le fait en conformité avec ses obligations légales, contractuelles et éthiques et en toute transparence.

## 2. Objectif

Cette politique définit les exigences et les éléments de notre programme mondial de protection de la confidentialité des données afin de garantir notre conformité aux obligations légales et

## 4. Principes fondamentaux du traitement des données personnelles

Entrust respecte les principes fondamentaux suivants lors du traitement des données personnelles :

- **Conformité à la loi et adéquation** : nous veillons à ce que les données personnelles soient collectées dans un but licite et qu'elles soient pertinentes et nécessaires à cette fin.
- **Précision et conservation**

Entrust ne supprime pas les copies des données personnelles de ses supports de sauvegarde et de ses serveurs à la fin de la période de conservation lorsque c'est irréalisable d'un point de vue commercial ; toutefois, les données personnelles ainsi conservées par Entrust sont protégées par les mêmes normes de sécurité que celles qui protègent les données personnelles lorsqu'elles sont utilisées. Les données personnelles restent soumises à la confidentialité et ne peuvent être consultées que dans la mesure où la loi en vigueur l'exige.

## 7.3 Effacement ou destruction des données personnelles

La politique mondiale de gestion des dossiers et la norme de traitement et de classification des informations définissent les exigences relatives au traitement approprié de tous les types de dossiers à la fin de la période de conservation prescrite.  En particulier, les principes suivants s'appliquent aux dossiers contenant des données personnelles :

- Les données

- garantit le rétablissement de l'accès aux données personnelles en temps utile en cas d'incident physique ou technique ;
- teste, évalue et analyse régulièrement l'efficacité des mesures techniques et organisationnelles mises en place pour sécuriser les données personnelles ;
- applique des normes de sécurité physique exigeant que les bureaux et les armoires soient fermés à clé s'ils contiennent des données personnelles, que les moniteurs/écrans individuels ne permettent pas aux passants de voir les données personnelles affichées et que les appareils électroniques (ordinateurs, tablettes, etc.) soient verrouillés ou déconnectés des systèmes de la Société lorsqu'ils sont laissés sans surveillance.

Pour évaluer les mesures de sécurité appropriées, Entrust prend en compte les risques associés au traitement des données, en particulier les risques de destruction accidentelle ou illégale, de perte, d'altération, de divulgation non autorisée ou d'accès aux données personnelles traitées.

Lorsqu'Entrust fait appel à des tiers pour traiter des données personnelles en son nom, ceux-ci le font sur la base d'instructions écrites d'Entrust et dans le respect des dispositions contractuelles (DPA, par exemple) pour traiter de manière appropriée les données personnelles

équivalentes aux propres exigences d'Entrust en matière de sécurité. Les données personnelles ne sont pas partagées en dehors d'Entrust si ces mécanismes ne sont pas en place. Divers outils de sécurité (DLP, par exemple) sont en place pour garantir que les données personnelles ne quittent pas l'organisation sans autorisation.

## 8.2 Test

Les données personnelles ne peuvent pas être utilisées dans les environnements de test d'Entrust sans exception de sécurité formelle approuvée à l'avance. Tous les environnements de test doivent respecter les normes et les contrôles applicables aux environnements de production et toutes les données personnelles dont l'utilisation a été approuvée dans les

norme relative au cycle de vie de développement sécurisé de logiciels (SDLC) fournit davantage de détails.

## 8.3 Signaler un incident de données personnelles

Un incident lié aux données personnelles peut prendre de nombreuses formes, y compris, mais sans s'y limiter :

- perte d'un appareil mobile ou d'un fichier papier contenant des données personnelles (par exemple, lorsqu'un appareil est oublié dans les transports en commun) ;
- vol d'un appareil mobile ou d'un fichier papier contenant des données personnelles ;
- erreur humaine (par exemple, un collaborateur envoie par erreur un e-mail contenant des données personnelles, ou modifie ou supprime accidentellement des données personnelles) ;

## 9. Transparence

Entrust assure la transparence de son programme mondial de confidentialité des données par le biais de pages de renvoi internes et externes robustes.

## 9.1 Avis de confidentialité

Entrust informe les personnes concernées du traitement de leurs données personnelles en tant que contrôleur et processeur de données. Ces informations sont disponibles dans les divers avis de confidentialité d'Entrust destinés aux utilisateurs du Web, aux candidats à l'emploi et aux collaborateurs, ainsi que dans les avis de confidentialité de chacun de ses produits, disponibles ici