POLITIQUE GLOBALE DE PROTECTION DES DONNEES PERSONNELLES

Classification	Publique
Version du document	2.0
Date de publication	26 février 2026

Table des matières

1. Introduction

Entrust Corporation et ses filiales (collectivement, « Entrust » ou la « Société ») traitent les données personnelles relatives à nos employés et aux contacts commerciaux de nos partenaires de vente, fournisseurs et clients en notre qualité de contrôleur des données. Entrust traite également les données personnelles relatives aux employés et aux utilisateurs finaux de ses clients en tant que sous-traitant des données. Lorsque Entrust traite des données personnelles, nous le faisons en conformité avec nos obligations légales et contractuelles et en toute transparence.

2. Objectif

Cette politique énonce les exigences et les éléments de notre programme mondial de confidentialité des données qu'Entrust a mis en place pour s'assurer que nous respectons les obligations légales et contractuelles pertinentes ainsi que les exigences en matière de certification et d'audit. La présente politique s'applique globalement à tous les traitements de données personnelles effectués par Entrust.

3. Définitions

« Contrôleur de données » désigne l'entité qui détermine la nécessité et les moyens de traitement des données personnelles et a la même signification que celle attribuée au « Processeur de PII » selon l'ISO 27701.

« Sous-traitant des données » désigne l'entité qui traite les données personnelles pour le compte du contrôleur de données et a la même signification que celle attribuée au « Processeur de PII » selon l'ISO 27701.

« Analyse d'impact relative à la protection des données (AIPD) » désigne une analyse documentée réalisée par un contrôleur de données ou un responsable du traitement des données qui évalue les risques pour la vie privée lorsque le traitement est susceptible d'entraîner un risque élevé pour les droits et libertés de la personne concernée.

Les « **Lois sur la protection des données** » désignent toutes les lois et réglementations applicables à Entrust en matière de protection des données personnelles et de confidentialité, y compris, sans s'y limiter, le Règlement général sur la protection des données (RGPD) de l'Union européenne, le Règlement général sur la protection des données (RGPD britannique) du Royaume-Uni, la loi britannique sur la protection des données (DPA 2018), la loi fédérale suisse sur la protection des données (telle que mise en œuvre le 1er septembre 2023) (FADP), la loi canadienne sur la protection des renseignements personnels et les documents électroniques (PIPEDA), la loi japonaise sur la protection des informations personnelles (APPI), la loi chinoise sur la protection des informations personnelles (PIPL) et les lois américaines sur la confidentialité, dans chaque cas telles qu'elles peuvent être modifiées, remplacées ou abrogées.

« Personne concernée » désigne l'individu identifié ou identifiable ou le ménage auquel se rapportent les données personnelles et a la même signification que celle attribuée au « Processeur de PII » selon l'ISO 27701.

« Analyse de l'impact du transfert de données » désigne une analyse documentée par un contrôleur ou un sous-traitant des données concernant l'impact et les implications en matière de sécurité d'un transfert de données personnelles de l'EEE ou du Royaume-Uni vers un pays situé en dehors de l'EEE/du Royaume-Uni qui n'a pas fait l'objet d'une décision d'adéquation de la part de la Commission européenne ou de l'Information Commissioner's Office.

« Analyse d'impact de l'intérêt légitime » désigne une analyse documentée réalisée par un contrôleur ou un sous-traitant des données afin de déterminer si l'intérêt légitime peut être utilisé comme base juridique pour le traitement des données personnelles. L'évaluation comprend un test à trois volets analysant si le traitement des données personnelles poursuit un intérêt légitime, s'il est nécessaire à cette fin et si les intérêts de la personne concernée l'emportent sur l'intérêt légitime.

« Données Personnelles » ou « PII » désigne les informations qui sont définies comme « informations personnellement identifiables », « informations personnelles » ou termes équivalents selon les lois sur la protection des données.

« Incident de données personnelles » désigne les événements qualifiés d'« incident de sécurité », de « violation de sécurité » ou de « violation de données personnelles », ou des termes équivalents tels que définis par les lois sur la protection des données et inclut toute situation dans laquelle Entrust prend connaissance d'un accès, d'une divulgation, d'une modification, d'une perte, d'une destruction ou d'une utilisation non autorisée de données personnelles.

« Traitement » signifie toute opération ou ensemble d'opérations effectuées sur des données personnelles, que ce soit par des moyens automatiques, telles que la collecte, l'enregistrement, l'organisation la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la divulgation par transmission, la diffusion ou toute autre mise à disposition, le rapprochement ou la combinaison, la restriction, l'effacement ou la destruction. Le traitement comprend également le transfert ou la divulgation de données personnelles à des tiers.

« Données personnelles sensibles » est un sous-ensemble des données personnelles et fait référence aux informations concernant une personne concernée qui, si elles sont perdues, compromises, consultées ou divulguées de manière inappropriée, pourraient causer un préjudice, un embarras, un désagrément ou une injustice à la personne concernée et sont donc soumises à une protection accrue.

« Données de catégorie spéciale » est un sous-ensemble des données personnelles et fait référence aux informations concernant l'origine raciale ou ethnique d'une personne, ses opinions politiques, ses croyances religieuses ou philosophiques, ou son appartenance à un syndicat, ainsi qu'au traitement des données génétiques, des données biométriques aux fins de l'identification unique d'une personne physique, des données relatives à la santé ou des données relatives à la vie sexuelle ou à l'orientation sexuelle d'une personne physique.

4. Principes fondamentaux du traitement des données personnelles

Entrust adhère aux principes fondamentaux suivants lorsqu'elle traite des données personnelles en tant que contrôleur de données :

- **Légalité et adéquation** : nous veillons à ce que les données personnelles soient collectées dans un but légitime et limitées à ce qui est pertinent et nécessaire à cette fin.
- **Précision et rétention** : Nous tenons nos systèmes à jour, fournissons des mécanismes permettant de mettre à jour les données personnelles inexactes et ne conservons pas les données personnelles plus longtemps qu'il n'est nécessaire pour atteindre l'objectif légal du traitement.
- **Confidentialité et intégrité** : nous veillons à ce que les données personnelles restent sécurisées et protégées pendant le traitement, mais nous réagissons rapidement et de manière appropriée aux incidents liés aux données personnelles s'ils se produisent, y compris en fournissant des notifications opportunes, le cas échéant.
- **Équité et transparence** : nous informons de manière adéquate les personnes concernées lorsque nous traitons leurs données personnelles. Nous expliquons clairement pourquoi nous avons besoin de ces informations, comment nous les utiliserons et comment elles seront traitées et protégées. Nous fournissons des mécanismes permettant aux personnes concernées d'exercer les droits qu'elles ont sur leurs données à caractère personnel en vertu de la législation applicable.

Tous les employés d'Entrust sont responsables du traitement et de la protection appropriés des données personnelles et comprennent que tout manquement à cet égard risque non seulement de miner la confiance des clients envers Entrust, mais aussi d'entraîner des amendes et des pénalités importantes pour l'entreprise.

5. Registres de traitement

Pour garantir la conformité avec les lois applicables en matière de protection des données et respecter notre engagement de transparence et de responsabilité, Entrust tient un registre des activités de traitement (RoPA) conformément à l'article 30 du RGPD et à d'autres réglementations pertinentes en matière de protection de la vie privée. L'APR comprend toutes les activités de traitement impliquant des données personnelles classées conformément à la norme de classification et de traitement des données d'Entrust.

6. Légalité et adéquation

6.1 Bases légales pour le traitement des données personnelles

Lorsqu'elle agit en tant que contrôleur de données, la société ne traite les données personnelles que dans la mesure où cela est légalement autorisé. Entrust s'appuie principalement sur les bases juridiques suivantes pour le traitement :

- Exécution d'un contrat ;
- Conformité aux obligations légales, y compris, mais sans s'y limiter, aux demandes légales des autorités judiciaires ;
- Intérêt légitime, sauf lorsque cet intérêt est surpassé par les intérêts ou les droits et libertés fondamentaux de la personne concernée ;
- Consentement.

Lorsque le consentement est la base juridique du traitement, Entrust s'assure que le consentement est librement donné, spécifique, éclairé et qu'il indique sans ambiguïté les souhaits de la personne concernée. La personne concernée a le droit de retirer son consentement à tout moment et pour n'importe quelle raison.

6.2 Analyses de la protection de la vie privée

6.2.1 Analyse de la protection de la vie privée dès la conception

Entrust évalue le traitement des données personnelles en fonction des principes fondamentaux décrits à la section 4 ci-dessus dans le cadre de la conception et de l'élaboration de produits nouveaux ou substantiellement modifiés et lors de l'intégration de solutions de fournisseurs où des PII seront traitées, y compris sous licence dans des applications logicielles de tierces parties. Cette analyse « de la protection de la vie privée dès la conception » est intégrée dans les processus de développement et d'intégration des fournisseurs d'Entrust. La réalisation de l'analyse nécessite l'examen et l'approbation des équipes chargées de la protection de la vie privée et de la sécurité de l'information d'Entrust. Le développement ne peut se faire sans approbation.

6.2.2 Analyse d'impact relative à la protection des données (AIPD)

Lorsque le traitement des données personnelles envisagé présente un risque élevé pour les droits et libertés d'une personne, Entrust réalise une AIPD pour documenter et évaluer l'objectif du traitement, la manière dont Entrust se conformera aux lois sur la protection des données et la manière dont l'entreprise atténuera les risques potentiels pour la personne concernée. Lorsqu'une AIPD se rapporte à un traitement pour lequel Entrust est le contrôleur des données, elle est examinée par le délégué à la protection des données d'Entrust qui doit approuver le traitement proposé avant qu'il ne commence. Les AIPD sont réexaminées et mises à jour au moins une fois par an, ou plus fréquemment si nécessaire, afin de garantir le maintien de la conformité avec les lois et règlements applicables.

6.2.3 Analyse d'impact des transferts des données (AITD)

Lorsque Entrust a l'intention de transférer des données personnelles de l'Espace économique européen (EEE) ou du Royaume-Uni vers un pays situé en dehors de l'EEE ou du Royaume-Uni qui ne bénéficie pas d'une décision d'adéquation de la Commission européenne ou du Bureau du commissaire à l'information du Royaume-Uni, Entrust remplit une AITD formelle pour analyser l'impact et les implications du transfert en termes de sécurité, en particulier lorsque les lois du pays destinataire pourraient permettre à son gouvernement d'avoir accès aux données personnelles transférées. Entrust ne procédera au transfert que si elle conclut que le risque posé par le transfert est acceptable. AITD il sera revu et mis à jour au moins une fois par an, ou plus fréquemment si nécessaire, afin d'assurer le respect continu des louis et règlementations applicables.

6.2.4 Analyse d'impact de l'intérêt légitime (AIIL)

Lorsque Entrust agit en tant que contrôleur des données et s'appuie sur l'intérêt légitime comme base juridique du traitement des données personnelles, l'entreprise effectue une analyse formelle de l'intérêt légitime pour documenter et évaluer l'intérêt légitime, déterminer si le traitement est nécessaire et évaluer si les intérêts, les droits et les libertés de la personne concernée l'emportent sur l'intérêt légitime ou le supplantent. Entrust ne procédera au traitement sur la base de l'intérêt légitime que si l'AIIL conclut que l'intérêt légitime n'est pas outrepassé.

6.2.5 Normes pour le traitement des données sensibles et de catégorie spéciale

En tant que contrôleur de données, Entrust traite des données personnelles sensibles concernant des employés dans divers systèmes commerciaux et certaines données limitées de catégorie spéciale sur une base volontaire et dans la mesure où la législation locale l'autorise. Des contrôles appropriés sont en place et décrits dans les AIPD applicables, la norme de contrôle d'accès pour les données sensibles et de catégorie spéciale, et une formation renforcée à la protection de la vie privée est obligatoire pour les employés qui traitent ces données sensibles et de catégorie spéciale.

6.2.6 Règle des données en vrac

Les données personnelles sensibles, y compris les données « omiques » humaines, les identifiants biométriques, les données de géolocalisation précises, les données personnelles relatives à la santé, les données financières personnelles et certains identifiants personnels des citoyens américains, ainsi que les données du gouvernement américain, y compris les données de géolocalisation précises pour toute zone spécifiquement désignée comme présentant un risque accru d'exploitation (telles que les installations militaires, les installations de sécurité nationale, de défense ou de renseignement, ou les lieux de travail du personnel fédéral chargé du renseignement national), sont soumises à des restrictions en matière d'exportation, de transfert et d'accès. Ces données ne peuvent être fournies à aucune personne physique ou morale située dans un « pays à risque », contrôlée par celui-ci ou agissant sous ses ordres. Actuellement, les « pays à risque » sont la Chine (y compris Hong Kong et Macao), Cuba, l'Iran, la Corée du Nord, la Russie et le Venezuela.

Bien qu'un tel transfert ou accès puisse être fourni dans certaines circonstances, Entrust a décidé de ne pas s'engager dans des transactions avec des pays à risque qui impliquent des données personnelles américaines sensibles ou des données du gouvernement américain. Ces données ne devraient jamais être transférées à un pays à risque ou à une personne ou entité située dans un pays à risque, que ce soit par Entrust ou par toute personne agissant au nom d'Entrust.

6.3 Protections contractuelles

6.3.1 Accord de transfert de données intra-groupe (IGDTA)

Entrust Corporation et ses filiales concluent l'accord de transfert de données intra-groupe pour s'assurer que lorsque des données personnelles sont partagées au sein du groupe Entrust, elles sont couvertes par des clauses de partage de données appropriées (y compris des clauses contrôleur - sous-traitant comme l'exige le RGPD). L'IGDTA garantit également la mise en place de garanties appropriées (c'est-à-dire des clauses contractuelles types) lorsque le partage de données personnelles au sein du groupe Entrust implique le transfert de données personnelles de l'EEE/du

Royaume-Uni vers un pays situé en dehors de l'EEE/du Royaume-Uni qui ne bénéficie pas d'une décision d'adéquation de la Commission européenne ou de l'Information Commissioner's Office.

6.3.2 Accord de traitement des données (ATD)

Les entreprises extérieures au groupe Entrust qui traitent des données personnelles pour Entrust ou en son nom sont tenues de conclure un accord de traitement des données avec Entrust pour s'assurer que le tiers (par exemple, un vendeur, un fournisseur, un partenaire de distribution) a mis en place des mesures techniques et organisationnelles appropriées pour se conformer aux lois pertinentes sur la protection des données. Entrust prend des engagements équivalents vis-à-vis de ses clients lorsqu'elle agit en tant que sous-traitant des données, par le biais d'un accord de traitement des données standard.

6.3.3 Dispositions générales en matière de confidentialité

Le langage contractuel relatif à la protection de la vie privée est également intégré dans les accords standard avec les clients, les fournisseurs et les partenaires, ainsi que dans l'accord de non-divulgation (NDA) standard d'Entrust. Les contrats avec les vendeurs et les fournisseurs prévoient également l'obligation de se conformer à la Règle des données en vrac.

7. Exactitude et conservation

7.1 Gestion des dossiers

Le programme global de gestion des dossiers garantit qu'une période de conservation est formellement définie pour le traitement des données personnelles afin de s'assurer qu'elles ne sont conservées que le temps nécessaire, et que les données personnelles sont effacées, détruites ou rendues anonymes à la fin de la période de conservation assignée. La politique globale de gestion des dossiers énonce les exigences relatives au traitement de tous les dossiers, et pas seulement de ceux contenant des données personnelles, et le calendrier de conservation des dossiers qui l'accompagne définit la période de conservation pour chaque type de dossier conservé par l'entreprise.

7.2 Stockage et sauvegarde des données personnelles

Entrust stocke et sauvegarde les données personnelles sur plusieurs sites de serveurs gérés directement et indirectement par l'entreprise. Les services informatiques et les fournisseurs concernés (pour les applications hébergées dans le cloud et non gérées par les services informatiques) reçoivent des conseils standard sur le traitement approprié des données personnelles sur ces serveurs, y compris en ce qui concerne le stockage et les sauvegardes.
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 cela serait commercialement impraticable ; toutefois, les données personnelles conservées par Entrust de cette manière sont protégées par les mêmes normes de sécurité que celles qui protègent les données personnelles lorsqu'elles sont utilisées, et les données personnelles restent soumises à la confidentialité et ne peuvent être consultées que dans la mesure où la loi applicable l'exige.

7.3 Effacement ou destruction des données personnelles

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

- Les données personnelles ne doivent pas être copiées, sauf si cela est nécessaire pour atteindre l'objectif spécifié pour le traitement, et toutes les copies effectuées doivent conserver toutes les marques originales de confidentialité ou de propriété.
- Les dossiers papier doivent être déchiquetés et éliminés en toute sécurité lorsqu'il n'est plus nécessaire de les conserver, et ne peuvent pas être éliminés par un autre moyen.
- Les données personnelles sous format électronique doivent être supprimées ou rendues anonymes dès qu'elles ne sont plus nécessaires.
- Le service informatique est responsable de la destruction ou de l'effacement des équipements électroniques contenant des données personnelles (par exemple, ordinateurs portables, ordinateurs de bureau, appareils mobiles appartenant à l'entreprise, et données professionnelles sur des appareils personnels apportés par les employés - BYOD) conformément aux politiques et normes de sécurité de l'information applicables.

8. Confidentialité et intégrité

8.1 Sécurité des informations

Lorsque l'entreprise traite des données personnelles, elle prend des mesures appropriées pour garantir que ces données restent sécurisées et sont protégées contre tout traitement non autorisé ou illégal, ainsi que contre la perte accidentelle, la destruction ou les dommages. Entrust applique ces mesures comme suit :

- Chiffrer les données personnelles au repos et en transit lorsque la loi ou le contrat l'exige et, en outre, dans la mesure où cela est commercialement possible ;
- Garantir la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et services utilisés pour traiter les données personnelles grâce à des plans formalisés de reprise des activités et de reprise après sinistre qui sont régulièrement testés ou mis à l'épreuve ;
- Garantir le rétablissement de l'accès aux données personnelles de manière rapide en cas d'incident physique ou technique ;
- Tester, évaluer et apprécier périodiquement l'efficacité des mesures techniques et organisationnelles mises en place pour sécuriser les données personnelles ;
- Des normes de sécurité physique sont en place et exigent que les bureaux et les placards soient fermés à clé s'ils contiennent des données personnelles, que les écrans individuels ne permettent pas aux passants de voir des données personnelles et que les appareils électroniques (ordinateurs, tablettes, etc.) soient verrouillés ou déconnectés des systèmes de l'entreprise lorsqu'ils sont laissés sans surveillance.

Lors de l'évaluation des contrôles de sécurité appropriés, Entrust prend en compte les risques associés au traitement, en particulier le risque de destruction, de perte, d'altération, de divulgation non autorisée ou d'accès accidentel ou illégal aux données personnelles traitées.

Lorsque Entrust engage des tiers pour traiter des données personnelles en son nom, ces parties le font sur la base d'instructions écrites d'Entrust et sous réserve de dispositions contractuelles (par exemple, ATD) pour traiter de manière appropriée les données personnelles et mettre en œuvre des mesures techniques et organisationnelles appropriées qui sont au moins 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 (par exemple, DLP) sont en place pour garantir que les données personnelles ne quittent pas l'organisation sans autorisation.

8.2 Tests

Les données personnelles ne peuvent pas être utilisées dans les environnements de test d'Entrust sans une exception formelle de sécurité approuvée à l'avance. Tous les environnements de test doivent respecter les normes et les contrôles en vigueur pour les environnements de production et toutes les données personnelles dont l'utilisation a été approuvée dans les environnements de test doivent être supprimées sans délai une fois les tests terminés. Des détails supplémentaires sont présentés dans le cycle de vie du développement de logiciels sécurisés (S-SDLC).

8.3 Signaler un incident de données personnelles

Un incident concernant des 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, laisser accidentellement un appareil dans les transports en commun) ;
- Vol d'un appareil mobile ou d'un fichier papier contenant des données personnelles ;
- Erreur humaine (par exemple, un employé envoie accidentellement un e-mail contenant des données personnelles à un destinataire involontaire, ou modifie ou supprime accidentellement des données personnelles) ;
- Cyber-attaque (par exemple, ouverture d'une pièce jointe à un e-mail provenant d'un tiers inconnu contenant un ransomware ou d'autres logiciels malveillants) ;
- Autoriser l'utilisation/l'accès non autorisé (p. ex., permettre à un tiers non autorisé d'accéder aux zones sécurisées des bureaux ou des systèmes d'Entrust) ;
- Destruction physique et perte (par exemple, incendie ou inondation) ;
- Des informations sont obtenues auprès d'Entrust par un tiers par le biais de tromperie (par exemple, des attaques de phishing ou de smishing).

Un incident relatif aux données personnelles est susceptible de s'être produit s'il y a :

- Une ouverture de session inhabituelle et/ou une activité excessive du système concernant des comptes d'utilisateurs actifs ;
- Activité d'accès à distance inhabituelle ;
- La présence de faux réseaux sans fil (Wi-Fi) visibles ou accessibles depuis l'environnement de travail d'Entrust ;
- Une défaillance de l'équipement ;
- Enregistreurs de frappe matériels ou logiciels connectés ou installés sur les systèmes Entrust.

Les employés qui prennent connaissance ou qui ont des raisons de soupçonner qu'un incident impliquant des données personnelles a pu se produire ou est sur le point de se produire doivent immédiatement contacter le Centre des opérations de sécurité d'Entrust à l'adresse SOC@entrust.com.

8.4 Réponse aux incidents concernant les données personnelles

En cas d'incident réel ou imminent concernant des données personnelles, Entrust mettra en œuvre ses procédures d'intervention et de traitement des incidents maintenues par le service de sécurité de l'information afin de minimiser l'impact de l'incident et d'aviser les organismes de réglementation, les personnes concernées et/ou d'autres parties comme l'exige la loi et/ou le contrat. Une réponse comprendra généralement les éléments suivants :

- Enquêter sur l'incident pour déterminer la nature, la cause et l'étendue des dommages ou préjudices causés ou susceptibles d'être causés ;
- Mettre en œuvre les mesures nécessaires pour empêcher l'incident de continuer ou de se reproduire, et limiter les dommages aux personnes concernées ;
- Évaluer s'il existe une obligation de notifier d'autres parties (par exemple, les autorités nationales de protection des données, les personnes concernées, les parties contractuelles) et effectuer ces notifications dans les délais impartis ;
- Enregistrer les informations concernant l'incident relatif aux données personnelles et les mesures prises en réponse, y compris documenter les décisions de notifier ou de ne pas notifier les régulateurs ou les parties concernées.

9. Transparence

Entrust assure la transparence de son programme global de confidentialité des données par le biais de pages d'accueil interne et externe solides.

9.1 Avis de confidentialité

Entrust informe les personnes concernées du traitement de leurs données personnelles en tant que contrôleur des données et en tant que sous-traitant. Ces informations sont disponibles dans les divers avis de confidentialité d'Entrust destinés aux utilisateurs du web, aux candidats à l'emploi et

aux employés, ainsi que dans les avis de confidentialité de chacun de ses produits, disponibles ici. Ces avis fournissent des informations sur :

- Les types de données personnelles traitées par Entrust ;
- La finalité et la base juridique du traitement ;
- Tiers utilisés pour le traitement, le cas échéant ;
- Lieu et durée du traitement ;
- Tout transfert transfrontalier de données personnelles ;
- Durée du traitement ;
- Droits de la personne concernée ;
- Détails de tout processus d'intelligence artificielle/de prise de décision automatisée.

9.2 Formation

Entrust fournit aux employés une formation obligatoire annuelle sur les responsabilités en matière de protection des données. La présentation de la formation sur la confidentialité des données a lieu au moment de l'intégration et ensuite chaque année. En plus de la formation d'introduction à la protection des données destinée à tous les employés, Entrust impose l'achèvement annuel de la formation avancée sur la protection des données pour les employés qui traitent des données sensibles et des données de catégorie spéciale, ainsi que la formation Privacy by Design pour les employés impliqués dans le développement et la conception de produits et services logiciels. Entrust continue à développer et à déployer d'autres formations sur la confidentialité spécifiques aux fonctions selon les besoins.

9.3 Droits de la personne concernée

Lorsque Entrust traite des données personnelles, les personnes concernées disposent de certains droits en vertu des lois sur la protection des données. Bien que ces droits varient selon les juridictions, les personnes concernées ont généralement le droit de :

- Demander des renseignements sur les données personnelles qu'Entrust détient à leur sujet, y compris une copie de ces renseignements ;
- Faire rectifier les données personnelles inexactes les concernant et faire compléter les données personnelles incomplètes ;
- S'opposer au traitement de leurs données personnelles par Entrust lorsque la société agit dans le cadre de ses propres intérêts légitimes. Entrust peut continuer à traiter les données personnelles malgré une objection si les intérêts légitimes de la société l'emportent sur ceux de la personne concernée, ou si Entrust doit le faire pour des raisons légales ;
- Demander à Entrust de détruire les données personnelles détenues à l'égard de la personne concernée. La Société peut refuser cette demande si les données personnelles sont toujours nécessaires aux fins pour lesquelles elles sont traitées et qu'il existe une base légale pour qu'Entrust continue le traitement ;
- Demander à Entrust de limiter le traitement de leurs données personnelles à la simple conservation dans certaines circonstances.

Entrust évaluera les droits d'une personne concernée en vertu des lois sur la protection des données au cas par cas et suivra la procédure de demande des personnes concernées (DSR) pour déterminer comment répondre à une demande. En général, Entrust utilisera les droits d'une personne concernée en vertu du RGPD de l'UE comme référence pour traiter toutes les demandes et appliquera les droits supplémentaires disponibles en vertu des lois sur la protection des données applicables à la personne concernée, dans la mesure où ces droits lui sont plus favorables. Si une personne concernée exerce ces droits et qu'Entrust a divulgué les données personnelles en question à un tiers, la Société fera de son mieux pour s'assurer que le tiers se conforme également aux souhaits de la personne concernée.

Les personnes concernées souhaitant demander des informations sur les données personnelles qu'Entrust détient à leur sujet doivent le faire en soumettant une demande formelle de la personne concernée (DSR). Si des employés reçoivent une demande directement (que ce soit verbalement ou par écrit), la demande doit être immédiatement transmise à l'adresse suivante : privacy@entrust.com.

9.4 Autorités de contrôle

Les coordonnées des autorités de contrôle des données varient selon le site. La liste des autorités du Comité européen de la protection des données est disponible ici. Le Bureau de l'Information Commissioner's Office du Royaume-Uni (ICO) est disponible ici. Le Commissariat à la protection de la vie privée du Canada peut être contacté ici.

9.5 Délégué à la protection des données

Sauf indication contraire, le responsable de la protection des données d'Entrust est :

Mishcon de Reya LLP
Africa House, 70 Kingsway, Londres, WC2B 6AH, Royaume-Uni
DPO@mishcon.com

10. Conformité

Tous les employés et les travailleurs temporaires sont tenus de se conformer à cette politique. De plus, toutes les unités commerciales doivent s'assurer qu'elles ont mis en place des normes et procédures locales appropriées pour se conformer à cette politique et à la législation applicable en matière de confidentialité des données dans leur juridiction. Les violations de cette politique seront prises au sérieux et peuvent entraîner des mesures disciplinaires pouvant aller jusqu'au licenciement. La présente politique peut être mise à jour ou modifiée à tout moment.

11. Dérogations

Toute dérogation à la présente politique est exclue.

12. Propriété et historique des révisions

La présente politique relève du directeur de la protection de la vie privée et sera révisée chaque année.